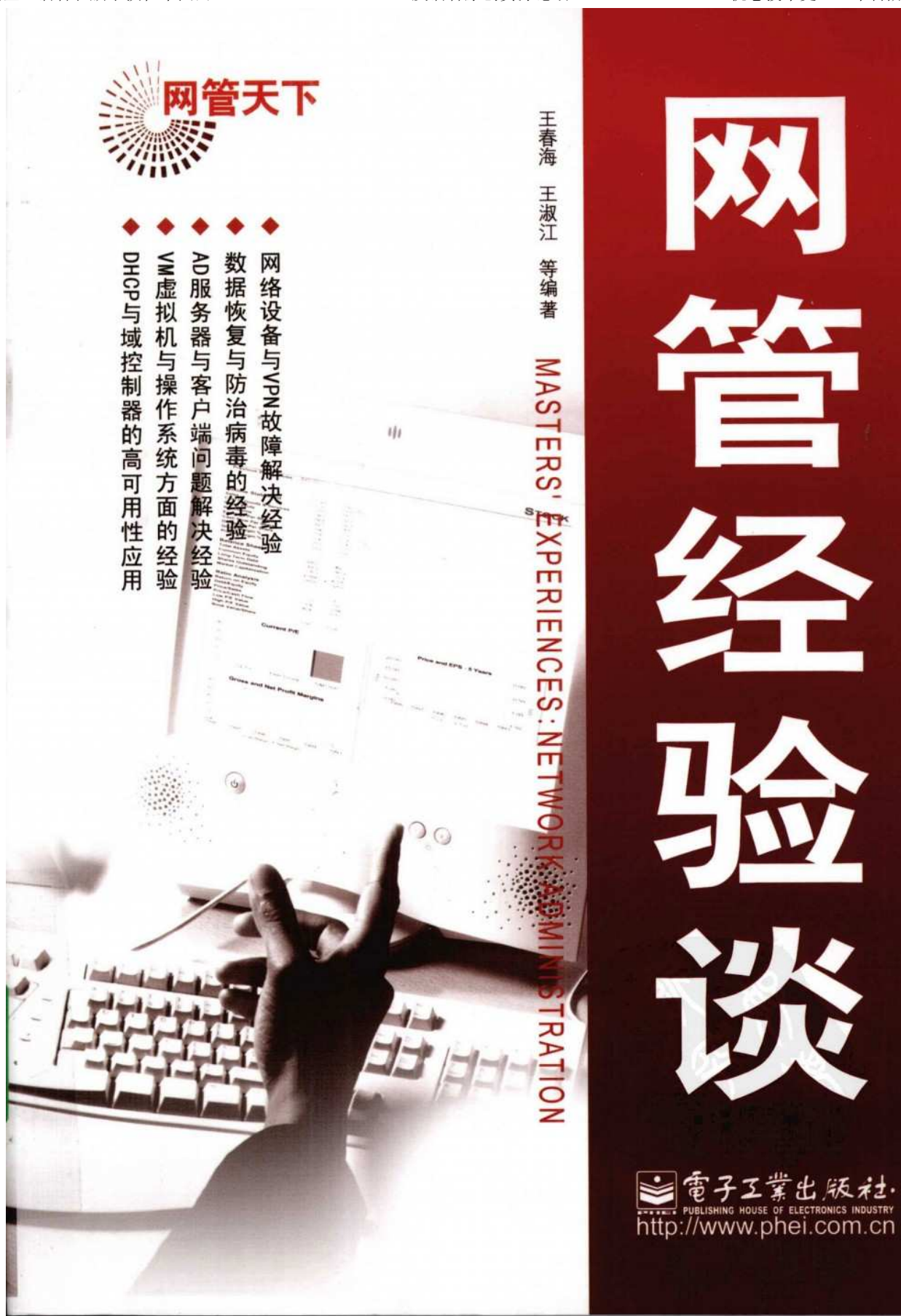


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



网络故障现场处理实践（第2版）
网络管理工具实用详解（第2版）
网络服务器应用深入实践（第2版）



网管经验谈

网络安全管理实践（第2版）
网络管理自动化
Linux服务器配置与管理

一套由国内资深网络专家写给网络建设与管理应用实践手册，能够全方位地解决网络建设与管理中的各种实际问题。

mixed media, -tɪ- [mɪksɪdɪə, -tɪ-] with a sing. verb) the use of several media, such as movies, TV, and lighting, especially for the purpose of entertainment.



天启星
<http://www.tqxbook.com.cn>

策划编辑：郭鹏飞
责任编辑：段春荣
责任美编：刘晓磊

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。



ISBN 978-7-121-09880-2



9 787121 098802 >

定价：59.80元

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客精神：

技術共享，資源共享，資料共享

不求最好，只求較好

做中國較好的網絡安全資料站

300G成套精品教程免费下载

每月网络期刊，黑客期刊发布

请将本站推荐给更多的好友

让大家都成为溜客一员

溜客資料共享群：

**访问溜客安全网最下方
查看本站最新共享QQ群**

溜客网络安全技术人才培养进行中

做一个通过正道可以养活自己的黑客

从我做起，不做伪黑客

WWW.176KU.COM/VIP.HTM

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录

C O N T E N T S

第 1 章 网络方面	1
1.1 网络基础经验	1
1.1.1 机房内网络设备布置经验	1
1.1.2 解决局域网 IP 冲突经验	4
1.1.3 网络打印机的安装经验	6
1.1.4 网上邻居疑难问题故障解决经验	8
1.1.5 局域网互访问题解决经验	10
1.1.6 网络命令全集	12
1.2 轻松上网的经验	18
1.2.1 快速修复 Windows Vista 不能连接网络的小经验	18
1.2.2 解决网络故障的方法总结	21
1.2.3 解决网络变慢的经验	25
1.3 路由器故障解决经验	27
1.3.1 交换机、路由器、集线器、网卡等网络设备的区别和联系	27
1.3.2 路由引起的网络故障排除经验	29
1.4 VPN 实用经验	32
1.4.1 VPN 网络解决方案小结	32
1.4.2 电子政务 VPN 应用案例分析	62
1.5 网络实验方面经验	63
1.5.1 修改 MAC 地址方法	63
1.5.2 虚拟局域网总结	66
1.5.3 百兆位至千兆位的网络升级经验	68
1.5.4 局域网加速方法小结	69
第 2 章 安全方面	73
2.1 计算机安全基础经验	73
2.1.1 如何保护计算机不中病毒的经验总结	73
2.1.2 使用 Net 命令检测网络安全的小经验	74
2.2 杀毒经典经验	78

v

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.2.1 杀毒小技巧	78
2.2.2 NOD32 3.0 客户端部署经验	81
2.3 防治 ARP 病毒的经验	85
2.3.1 关于 ARP 的一些知识小总结	85
2.3.2 关于防治 ARP 的一些经验	87
2.4 数据安全方面的经验	89
2.4.1 数据保护常识小总结	89
2.4.2 加密保证数据安全的总结	90
2.5 数据恢复方面的经验	91
2.5.1 保存数据的注意事项与数据恢复方法总结	91
2.5.2 误删除误分区的恢复经验	93
2.5.3 创建紧急修复磁盘	95
2.5.4 容灾所涉及的恢复技术	96
2.5.5 Windows Server 2003 的数据备份	98
第 3 章 服务器方面	105
3.1 AD 服务器方面的经验	105
3.1.1 快速创建大批量域用户的小技巧	105
3.1.2 快速更改公司 Windows 域名的方法	107
3.1.3 AD 复制的经验小结	114
3.2 服务器端问题解决经验	118
3.2.1 关于安装 SQL Server 2000 小经验	118
3.2.2 Windows Vista 自动远程部署经验	120
3.2.3 解决 WSUS 服务器的几个问题的经验	129
3.2.4 发布内网中多台 FTP 服务器的经验	131
3.2.5 用 Hotmail 空间组建自己的邮件系统的经验	137
3.3 客户端问题解决经验	148
3.3.1 解决 OCS 2007 不能自启动的小经验	148
3.3.2 关于使用 WSUS 时客户端导入注册表文件的解决方法	151
3.4 增强服务器功能的经验	157
3.4.1 App-V 使用经验	157
3.4.2 域环境安装企业根 CA 经验	170
3.4.3 使用 RMS 保护企业 Word 文档	176
3.5 轻松管理服务器的经验	193
3.5.1 轻松实现智能化身份验证	193

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.5.2	手工删除父子域信任关系经验	217
3.5.3	DNS 服务调教经验	219
3.6	服务器安全管理经验	221
3.6.1	防范服务器被添加隐藏账户的小经验	222
3.6.2	限制域用户的并发登录的小经验	225
3.6.3	3389 端口修改	226
3.6.4	Windows 2003 内置的防火墙设置经验	229
3.6.5	Windows Server 2003 R2 批量许可产品密钥加密	231
第 4 章	网管员业余管理经验	233
4.1	网络管理员的基础经验	233
4.1.1	DOS 命令全集	233
4.1.2	DOS 批处理文件	241
4.1.3	限制上外网的经验	256
4.2	网络管理工具使用经验	263
4.2.1	使用“云端软件平台”的经验	263
4.2.2	聚生网管使用经验	272
4.2.3	制作 Windows Server 2008 中文版的经验	274
4.2.4	利用 Win XP 自带工具实现远程管理	279
第 5 章	虚拟化应用方面	281
5.1	虚拟化产品及应用举例	281
5.1.1	虚拟化应用总结	281
5.1.2	证券公司 Netware 服务器故障解决方案	309
5.1.3	轻松打造潜行者活动硬盘电脑	313
5.2	VM 虚拟机的使用经验	325
5.2.1	关于 VM 虚拟机虚拟网卡问题的小结	325
5.2.2	在虚拟机中测试 U 盘量产的小经验	328
5.2.3	轻松实现 VMware 与主机同步开关机	334
5.3	使用 VM 做实验的经验	335
5.3.1	VMware License Server 使用经验	335
5.3.2	一台主机实现做广域网实验的方法	341
5.3.3	在 VMware Workstation 虚拟机中安装 VMware ESX 3I 的经验	357

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 章 操作系统方面	369
6.1 计算机故障解决经验	369
6.1.1 计算机无法启动故障解决经验	369
6.1.2 电脑黑屏解决方法	370
6.1.3 Windows 蓝屏错误代码小结	377
6.1.4 电脑故障排除经验	381
6.2 操作系统方面问题解决经验	383
6.2.1 内存不能够读写问题的分析与解决	383
6.2.2 虚拟内存不足的原因汇总及解决方法	387
6.2.3 Windows 命令行下的进程管理小经验	389
6.2.4 Windows 系统中常用进程解析小结	391
6.2.5 修改应用程序访问权限经验	393
6.3 服务器操作系统使用方面的经验	399
6.3.1 将 Windows Server 2003 升级到 Windows Server 2008	400
6.3.2 Windows Server 2008 标准证书使用经验	403
6.3.3 体验 Windows2008 新功能——Server Core 的安装和配置	419
第 7 章 高可用性应用	427
7.1 磁盘高可用性	427
7.1.1 常见 Raid 类型	427
7.1.2 BIOS 设置 Raid 卡	434
7.2 网卡高可用性	436
7.2.1 网卡数量	437
7.2.2 多网卡优点	437
7.2.3 部署虚拟网卡	437
7.3 DHCP 高可用性应用建议	441
7.3.1 DHCP 容错 50/50 故障转移	441
7.3.2 DHCP 容错 80/20 故障转移	441
7.3.3 DHCP 容错 100/100 故障转移	442
7.3.4 待机作用域	442
7.3.5 群集服务	442
7.4 域控制器高可用性	442
7.4.1 域控制器概述	442
7.4.2 部署域控制器	444

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.4.3 额外域控制器	452
7.4.4 管理域控制器	459
7.4.5 AD DS 域服务故障	471
第 8 章 网络防病毒系统	481
8.1 防病毒现状	481
8.1.1 病毒传播途径分析	481
8.1.2 网络病毒传播过程分析	482
8.1.3 主动防御	483
8.1.4 被动防御	484
8.1.5 网络防病毒体系实现的目标	485
8.2 部署 WSUS 系统更新	486
8.2.1 部署环境	486
8.2.2 系统补丁部署原则	488
8.2.3 部署 WSUS 服务器注意事项	489
8.2.4 部署客户端计算机系统更新注意事项	494
8.3 部署应用层防火墙	499
8.3.1 允许用户访问 Internet	500
8.3.2 禁止扩展名类型下载	502
8.4 部署隔离服务器	504
8.4.1 部署隔离服务器	504
8.4.2 配置网络隔离策略	511
8.5 部署防病毒系统	518
第 9 章 用户、计算机账户管理	519
9.1 组织单位管理	519
9.1.1 组织单位和组的区别	519
9.1.2 组织单位规划	519
9.1.3 创建组织单位	524
9.2 组管理	526
9.2.1 组分类	527
9.2.2 组作用域	527
9.2.3 组部署原则	528
9.2.4 常用组管理任务	530
9.3 用户管理	534

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 9.3.1 注意事项..... 534
 - 9.3.2 用户生命周期..... 536
- 9.4 计算机账户管理..... 566
 - 9.4.1 注意事项..... 566
 - 9.4.2 计算机账户生命周期..... 570
- 参考文献.....574



第1章 网络方面

计算机网络在我们的日常生活中已经变得越来越普遍。特别是 20 世纪 90 年代以来，随着 Internet 在世界范围的普及，计算机网络逐渐成为人们获取信息、发布信息的重要途径，与此同时，基于计算机网络的应用也越来越多，许多人们生活中的重要环节都可以利用网络方便、快捷地实现。

本章主要介绍了五个方面的经验：网络基础经验、轻松上网经验、路由器故障解决经验、vpn 实用经验，以及网络实验方面经验。

1.1 网络基础经验

本节主要介绍了五个基础性的网络经验，包括机房内网络设备布置经验、解决局域网 IP 冲突经验、网络打印机安装经验、网上邻居疑难问题故障解决经验、局域网互访问问题解决经验，另附网络命令全集，以供初级网络管理员查询使用。

1.1.1 机房内网络设备布置经验

要组建一个网络，不仅要从自身的实际需求出发，根据组网经费的多少来务实地规划与设计网络；还要在采购好网络设备和服务器等设备后，对机房、办公地点进行合理的网络布局与布线。对于网管员来说，怎样去进行网络布局与布线这项工作才是至关重要的。

本书所说的网络布局主要是指机房里的网络设备和服务器等设备如何放置，它们又与网络布线如何协调。

1. 网络布局的原则

(1) 实用性。

企业组建的局域网应当根据机房的面积大小、设备的数量多少等情况来决定如何具体实施，根据网络布线的特点来发挥网络布局实用性是非常重要的。

(2) 全面性。

组网过程中，进行网络布局时要考虑周全，尽量让各种设备和布线系统处于合理的位置。

(3) 可靠性。

局域网无论怎样布局，最终目的是要保证其中的所有设备都能可靠稳定地运行，从而使网络能够正常运转。

(4) 便于维护与升级。

网络的组网不是一成不变的，随着 IT 企业业务不断发展的需求，原先组建的局域网也需要不断地完善和扩充；规划网络布局时就应该考虑到以后的网络维护与升级操作。

■ 2. 网络布局的具体实施要求

规划网络布局首先要规划与设计好机房的设备布局和布线系统，使其合理搭配，然后再全面地考虑网络的布局。

为了确保网络、计算机系统稳定、安全、可靠地运行，保障机房工作人员有良好的工作环境，机房的规划与设计应该做到技术先进、经济合理、安全适用、确保质量，符合国家的有关规定。

（1）防静电。

静电不仅会使计算机运行出现随机故障，而且还会导致某些元器件、双极性电路等的击穿和毁坏。此外，还会影响操作人员和维护人员的正常工作和身心健康。

（2）防火、防盗。

机房的设计要重点考虑消防灭火方面的功能。在设计时可以根据消防的防火级别来确定机房的设计方案，机房的火灾报警系统要求在一楼设有值班室或监控点。

机房里应注意防盗设施的安装，具体地可采用防盗门、防盗锁、警卫、自动报警系统等。

（3）防雷。

由于机房的通信和供电电缆大多是从室外引入机房，容易遭受雷电的侵袭，因此机房建筑的防雷设计尤其重要。如计算机通信电缆的芯线、电话线等均应加装避雷器。

（4）保温。

机房里的湿度以保持在 20%~80% 的范围为宜，而温度则应保持在 15℃~35℃。安装空调来调节温度是解决此问题的最好办法。

■ 3. 布线系统的规划与设计

有了好的机房，网络设备就有了好的“家”，组建的 IT 网络应当通过布线系统将机房和办公地点互联起来，确保网络的正常运行。如果企业的接入点较多，我们可以采取接入层、汇聚层、交换层三个网络层次的设计，并在此基础上进行布线系统。

对于接入层来说，选择一个合理的接入设备是最关键的，而且我们要根据接入的设备来选择合适的带宽。汇聚层是整个局域网的核心部分，汇聚层网络设备一般支持网络管理功能，方便我们的管理维护和以后的网络升级改造。交换层是整个网络的中间层，连接着汇聚层和网络结点，是决定我们整体网络传输质量的一个很重要的环节。随着百兆位网络设备的普及，我们建议交换层的网络设备首选百兆位。

布线是连接网络接入层、汇聚层、交换层和网络结点的重要环节。在布线时，最好使用专门的通道，不要与电源线、空调线等具有辐射的线路混合布线。

接入层与汇聚层之间的双绞线建议选择超五类屏蔽双绞线，这样可以使网络性能得到最大的提升。汇聚层与交换层之间的双绞线，由于是网络数据传输量最大的一个层次，同样采用超五类屏蔽双绞线。交换层与网络结点之间，我们就可以采用普通的超五类非屏蔽双绞线。

网络设备最好放在结点的中央位置，这样做既可以节约综合布线的成本，又提高了网络的整体性能和网络传输质量。值得注意的是虽然双绞线的传输距离是 100 m，但在 95 m 处才能获得最佳的网络传输质量。在做网络布线时，最好能够设计一个设备间，用来放置网络设备。

4. 网络布局的规划与设计

目前的网络设备大都采用机架式的结构（多为扁平式，或像个抽屉），如交换机、路由器、硬件防火墙等。这些设备之所以用这样一种结构类型，是因为它们都是按照国际机柜标准进行设计的，这样各种设备的平面尺寸就基本统一，可以把它们一起安装在一个大型的立式标准机柜中。这样做的好处非常明显：一方面可以使设备占用最小的空间，另一方面则便于与其他网络设备的连接和管理，同时机房内也会显得整洁、美观。

我们经常接触到的机房里放置有网络机柜、服务器机柜和综合布线柜，从这三个机柜的名字就可以看出它们各自所起的作用。

一般来说，网络设备（如交换机、路由器、防火墙、加密机等）以及网络通信设备（如光端机、调制解调器等）是放置在网络机柜的；服务器机柜的宽度为 19 英寸（1 in=25.4 mm），高度以 U 为单位（1 U=1.75 in=44.45 mm），通常有 1 U，2 U，3 U，4 U 几种标准的服务器。机柜的尺寸也是采用通用的工业标准，通常从 22 U 到 42 U 不等。机柜内按 U 的高度有可拆卸的滑动拖架，用户可以根据自己服务器的标高灵活调节高度，以存放服务器、集线器、磁盘阵列柜等设备。服务器摆放好后，它的所有 I/O 线全部从机柜的后方引出（机架服务器的所有接口也在后方），统一安置在机柜的线槽中，一般贴有标号，以便于管理。

综合布线柜一般配有前后可移动的安装立柱，可以自由设定安装空间，还可按需要配置隔板、风扇、电源插座等附件。配线架通常安装在机柜里，配线架的一面是 RJ45 口，其上标有编号；另一面是跳线接口，上面也标有编号，这些编号和上面的 RJ45 口的编号是一一对应的。每一组跳线都标识有棕、蓝、橙、绿的颜色，双绞线的色线要和这些跳线一一对应，这样进行操作时就不容易接错。配线架不仅仅是为了便于管理线对，而且可以防止串扰，增加线对的隔离空间，提供 360° 的线对隔离。

在机房中，必须放置交换机、功能服务器群和网络打印设备，以及局域网络连接 Internet 所需的各种设备，如路由器、防火墙和网管工作站等。因此机房的网络布局一般至少要有三个机柜，综合布线柜和网络机柜应当紧连在一起，便于调线操作，然后再考虑服务器机柜以达到网络设备和布线系统的布局合理。

在网络布局中，每个机柜内最好留点空间，便于以后网络设备、服务器设备的扩充，综合布线柜里除了网络布线外，还有可能布置电话线，所以要在机柜里留下一定空间。

从机柜内部线缆敷设的角度看，机柜配置密度更高，容纳的 IT 设备更多，大量采用冗余配件（如冗余电源、存储阵列等），机柜内设备配置频繁变换，数据线和电缆随时增减。所以，机柜必须提供充足的线缆通道，能从机柜顶部、底部进出线缆。在机柜内部，线缆的敷设必须方便、有序，与设备的线缆接口靠近，以缩短布线距离；减少线缆的空间占用，保证设备安装、调整、维护过程中，不受到布线的干扰，并保证散热气流不会受到线缆的阻挡；同时，在故障情况下，能对设备布线进行快速定位。

供电系统和制冷系统是计算机机房的两个重要部分。在供电系统中，一般采用在线的 UPS 供电方式，蓄电池实际可供使用的容量与蓄电池的放电电流大小、蓄电池的环境工作温度、存储时间的长短和负载的性质（电阻性、电感性、电容性）密切相关。

制冷系统（空调）涉及到机房的整个物理环境，包括空调、地板、机柜及房间布局等诸多方面；因此 UPS 和空调我们也要考虑将它们放置在一个合适的位置。如果机房空间较大，可以将 UPS 和空调都放在机房里；如果空间较小，可以把 UPS（包括蓄电池）放在配电房里。

网管天下 网管经验谈

需要注意的是如果大楼里安装有“中央空调”时，机房里也必须安装独立的空调，因为中央空调不可能 24 小时都开着，上班的时间可以利用中央空调，下班和星期节假日的时候，如果服务器、网络设备需要正常运行，则必须要开机房里的独立空调。

机柜的扩展性表现在机柜内设备密度的扩展和机柜数量的扩展，因此网络布局时必须将机柜的配风能力（通常称为散热能力）和配电能力考虑在内。一方面，机柜内的设备需要温度、湿度适宜并且风量充足的冷风（冷空气）。这些冷风被机柜内的 IT 设备吸入，从而为设备内的部件（尤其是 CPU）降温。当机柜内设备增加到一定数量时，由地板出风口送出的冷风风量将不能满足所有设备的需求，从而形成部分 IT 设备配风不足而过热。

解决机柜内设备密度扩展时遇到的这种局部热点问题可以采用调配 IT 设备位置的方式来解决。例如，把热负荷最大的设备安装在机柜中部位置，以便获得最大的配风风量。另外的解决方法是，在机柜的上部或下部位置安装轴向水平的强排风扇，增强上部或下部的吸入能力（即减小 IT 设备的入口静压），从而增加配风风量。

另一方面，机柜内的设备需要供电以及与机柜外部进行通信。当机柜内的 IT 设备数量增加时，这些线缆、连接端子同时成倍增加，从而对机架式电源排插的容量、插口数量都提出了扩展要求。机柜内的布线空间也是需要提前考虑的，因为当机柜内的功率密度提高时，设备后部的线缆将明显增加风阻，所以必须考虑线缆管理及走线空间的问题。

1.1.2 解决局域网 IP 冲突经验

要想避免 IP 地址冲突故障现象的发生，首先应该了解制造 IP 地址冲突的方法，只有这样才能对症下药，采取针对性措施来拒绝 IP 地址冲突“干扰”局域网的正常运行。

一般来说，在局域网投入运行的初期，网络管理员都会为局域网中的所有工作站分配一个合适的 IP 地址。不过，在局域网工作站长时间运行后，很可能会出现系统瘫痪或者其他一些故障现象，导致工作站的上网参数发生了丢失。此时工作站用户很可能会自己动手，进入本地工作站系统的 TCP/IP 属性设置窗口，在其中随意为本地工作站分配一个 IP 地址，该 IP 地址由于不是网络管理员事先划分好的那个 IP 地址，这样一来自然就会形成 IP 地址的冲突现象。在使用静态 IP 地址的局域网工作环境中，普通用户可以很容易地打开本地系统的 TCP/IP 属性设置窗口，并随意修改本地工作站的 IP 地址，从而造成 IP 地址使用出现混乱。

为了保护本地工作站的 IP 地址不被非法用户随意盗用，有一些熟悉网络的朋友往往会采取地址绑定的方法，将网络管理员事先分配给本地工作站的 IP 地址绑定到对应工作站的网卡设备上。这样一来即使非法用户盗用了本地工作站的 IP 地址，也不会干扰本地工作站的正常上网访问。可是，对于采取了绑定措施的 IP 地址来说，非法用户同样也能找到盗用的办法，那就是同时盗用合法工作站的 IP 地址与网卡设备的 MAC 地址，然后冒用合法主机的身份进行恶意破坏。

例如，非法用户在盗用了合法工作站的 IP 地址后，发现盗用后的 IP 地址不能正常连接到局域网网络中时，他们会认为该 IP 地址很可能被绑定了。于是非法用户尝试使用 MAC 地址扫描器之类的工具来查看、盗用合法工作站的网卡 MAC 地址，在盗取合法工作站的网卡 MAC 地址后，非法用户再将自己工作站的 IP 地址修改成合法 MAC 地址就可以了。修改网卡 MAC 地址的方法很简单，用户只要依次单击本地工作站系统桌面中的“开始”/“设置”/“网络连接”命令，在弹出的“网络连接列表”窗口中，用鼠标右键单击“本地连接”图标，从弹出的

快捷菜单中执行“属性”命令，打开本地连接属性设置对话框；单击该对话框中的“常规”选项卡，并在对应选项设置页面中单击“配置”按钮，进入本地工作站的目标网卡属性设置对话框；继续单击该设置对话框中的“高级”选项卡，打开如图 1-1 所示的高级选项设置页面，选中该设置页面左侧“属性”列表框中的“Network Address”选项，并将该选项的数值设置成盗用得来的网卡 MAC 地址，最后单击“确定”按钮就可以完成网卡物理地址的修改任务了。

了解制造 IP 地址冲突的几种方法后，用户就能根据不同的制造方法采取不同的阻止手段了。

在使用静态 IP 地址的局域网工作环境中，网络管理员可以使用 IP-MAC 地址绑定方法，也就是使用静态路由技术的方法来阻止普通工作站用户随意进入 TCP/IP 属性设置窗口，胡乱修改本地系统的 IP 地址。考虑到在相同的局域网网段中，普通工作站的网络寻径不是根据主机的 IP 地址而是根据主机的物理地址来进行的，在不同网段之间通信时才会根据主机的 IP 地址进行网络寻径，所以作为局域网网关的路由器设备上通常保存有 IP-MAC 的动态对应表，这是由 ARP 通信协议自动生成并维护的。我们可以进入局域网路由器的后台管理界面，从中找到配置 ARP 表的设置选项，对静态的 ARP 路由表进行个性化指定，日后局域网路由器设备会自动依照静态的 ARP 表检查通信数据包，要是无法对应，那么就不会进行数据转发操作。使用这种手段，网络管理员能够轻松地阻止非法攻击者在不修改网卡设备 MAC 地址的情况下，冒用合法工作站 IP 地址进行非法网络访问。

为了防止非法用户通过修改网卡 MAC 地址的方法来制造 IP 地址冲突故障现象，我们可以利用局域网交换机的端口绑定功能，来有效化解非法用户通过修改网卡 MAC 地址的方法来适应静态 ARP 表的问题。常见的可管理交换机都支持端口绑定功能，我们可以利用该功能提供的端口地址过滤模式，来实现阻止 IP 地址冲突的目的，因为交换机的端口地址过滤模式会允许每一个交换机的连接端口仅允许具有合法 MAC 地址的工作站访问网络，任何具有不合法 MAC 地址的工作站都将被交换机拒绝访问网络。

在组网规模较大的工作环境中，我们还可以通过划分虚拟子网的方法，来阻止 IP 地址冲突现象的发生。从严格意义上来说，划分虚拟工作子网其实并不属于技术措施，而是管理措施与技术措施结合在一起的手段。将那些具有相同访问行为的 IP 地址统一划分到相同的虚拟工作子网中，并正确设置好相关的路由策略，这样一来我们就能有效拒绝非法攻击者盗用其他工作子网 IP 地址现象的发生。

此外，我们在管理、维护局域网的过程中，尽量少用那些直接针对 IP 地址授权的管理模式，而应该综合运用加密、口令、VPN 连接或其他身份认证机制，建立多层次的严密的安全体系，那样一来就能有效降低 IP 地址冲突所带来的安全威胁了。

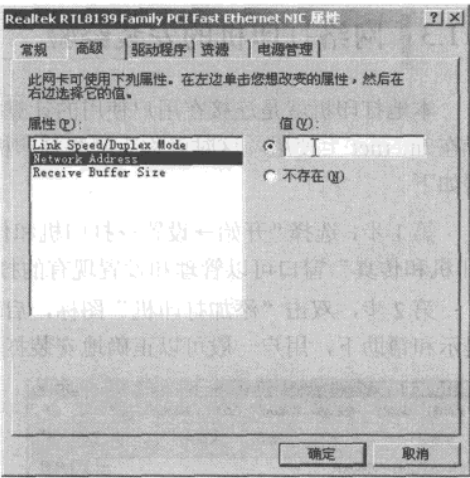


图 1-1 高级选项设置

1.1.3 网络打印机的安装经验

本地打印机就是连接在用户使用的计算机上的打印机。将其共享后可以在局域网内使用或者在 Internet 上使用，这时就称为网络打印机。要在 Windows 2003 Server 中添加打印机，步骤如下。

第 1 步，选择“开始→设置→打印机和传真”命令，打开“打印机和传真”窗口，利用“打印机和传真”窗口可以管理和设置现有的打印机，也可以添加新的打印机，如图 1-2 所示。

第 2 步，双击“添加打印机”图标，启动“添加打印机向导”。在“添加打印机向导”的提示和帮助下，用户一般可以正确地安装打印机，如图 1-3 所示。

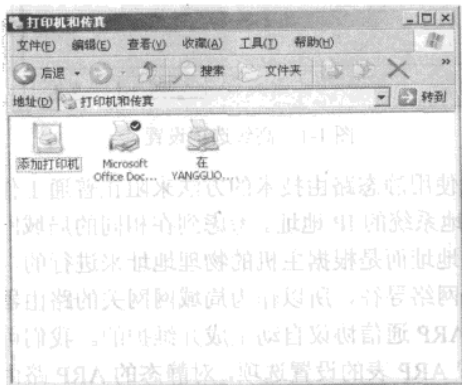


图 1-2 打印机和传真

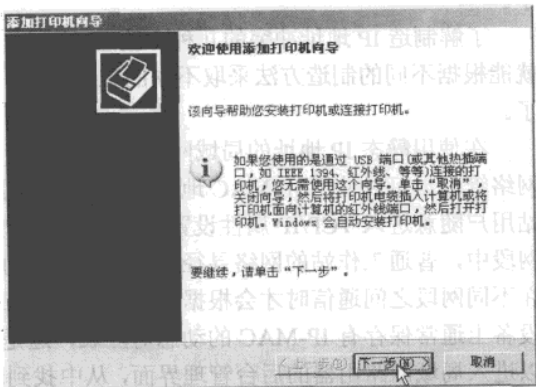


图 1-3 添加打印机向导

第 3 步，单击“下一步”按钮，进入“本地或网络打印机”对话框。在此对话框中，用户可选择添加本地打印机或者是网络打印机。选择“连接到此计算机的本地打印机”单选按钮，即可添加本机打印机，如图 1-4 所示。

第 4 步，单击“下一步”按钮，弹出“选择打印机端口”对话框，选择要添加打印机所在的端口。如果要使用计算机原有的端口，可以选择“使用以下端口”单选按钮。一般情况下，用户的打印机都安装在计算机的 LPT1 打印机端口上，如图 1-5 所示。

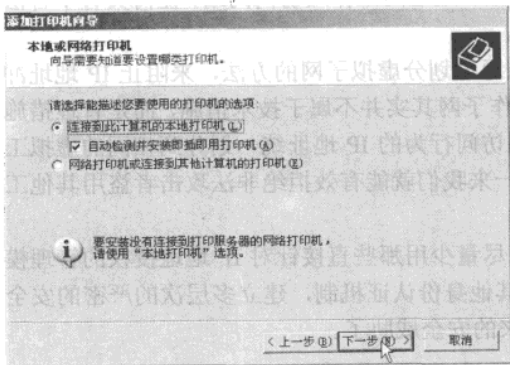


图 1-4 选择打印机类型

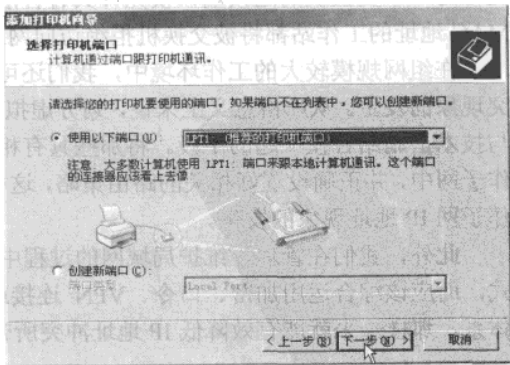


图 1-5 设置打印机端口

第 5 步，单击“下一步”按钮，弹出“安装打印机软件”对话框，选择打印机的生产厂商和型号。其中，“厂商”列表框列出了 Windows server 2003 支持的打印机的制造商，如图 1-6 所示。

如果在“打印机”列表框中没有列出所使用的打印机，说明 Windows server 2003 不支持该型号的打印机。一般情况下，打印机都附带有打印驱动程序。此时，用户可以单击“从磁盘安装”按钮，安装打印驱动程序即可。

第 6 步，单击“下一步”按钮，弹出“命名打印机”对话框。在该对话框中可以为打印机提交名称，如图 1-7 所示。

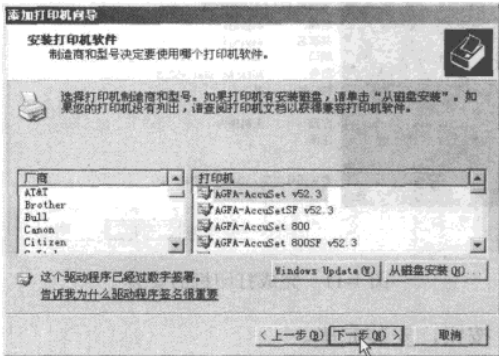


图 1-6 安装打印机向导

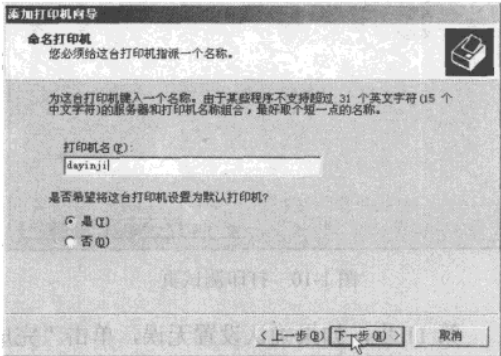


图 1-7 命名打印机

第 7 步，单击“下一步”按钮，弹出“打印机共享”对话框，如图 1-8 所示。
在这里设置其他计算机是否可以共享该打印机。如果选择“不共享这台打印机”单选按钮，那么用户安装的打印机只能被本机使用，局域网上的其他用户就不能使用该打印机。如果希望其他用户使用该打印机，可以选择“共享名”单选按钮，并在后面的文本框中输入共享时该打印机的名称，该打印机就可以作为网络打印机使用。这里选择“共享名”单选按钮，并在后面的文本框中输入共享时该打印机的名称。

第 8 步，单击“下一步”按钮，在弹出的窗口中要求用户提供打印机的位置和描述信息。可以在“位置”文本框中输入打印机所在的位置，让其他用户方便查看，如图 1-9 所示。

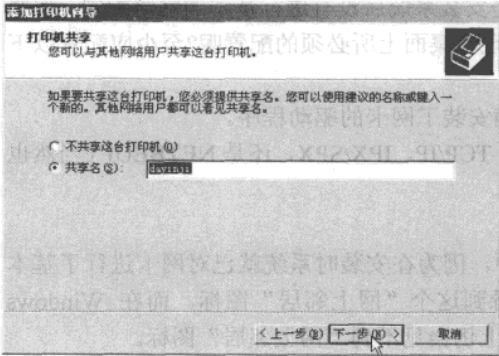


图 1-8 设置打印机共享名称

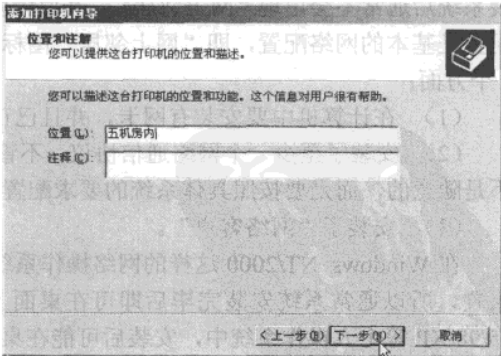


图 1-9 添加打印机描述

网管天下 网管经验谈

第 9 步，单击“下一步”按钮，在弹出的对话框中用户可以选择是否对打印机进行测试，来检查是否已经正确安装了打印机，如图 1-10 所示。

第 10 步，单击“下一步”按钮，在弹出“正在完成添加打印机向导”对话框中，显示了前几步设置的所有信息。如果有需要修改的内容，单击“上一步”按钮就可以返回到相应的位置修改，如图 1-11 所示。

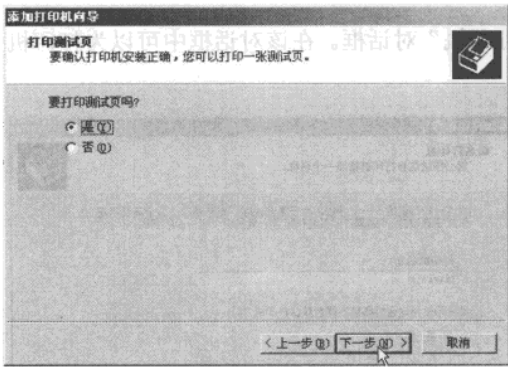


图 1-10 打印测试页

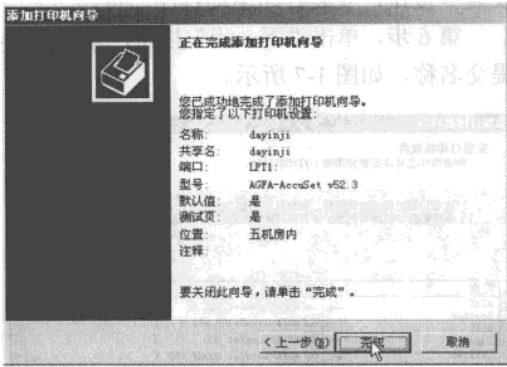


图 1-11 完成打印机的安装

第 11 步，如果确认设置无误，单击“完成”按钮，安装完毕。

1.1.4 网上邻居疑难问题故障解决经验

1. 桌面上“网上邻居”快捷方式图标丢失

这虽然是一种不很常见的故障，但却实实在在可能出现。如果没有“网上邻居”图标，就给网络访问带来了许多不便，毕竟用户已习惯了通过网上邻居访问网上其他计算机，尽管还有许多其他方式。

“网上邻居”的功能就是用来访问网络上其他计算机的，它只有在正确配置了基本的网络协议和服务后才会出现在桌面上，特别是安装了 Windows 95/98/Me 系统的计算机上，正常安装系统后通常不会出现“网上邻居”，其原因就是安装系统后没有进行基本的网络配置。哪些配置是基本的网络配置，即“网上邻居”图标出现在桌面上所必须的配置呢？至少应配置以下 3 个方面：

- (1) 在计算机中要安装有网卡，并且已正确安装了网卡的驱动程序。
- (2) 安装了至少一个网络通信协议，不管是 TCP/IP、IPX/SPX，还是 NETBEUI（当然也不是随意的，而是要按照具体系统的要求配置）。
- (3) 安装了“网络客户”。

在 Windows NT/2000 这样的网络操作系统中，因为在安装时系统就已对网卡进行了基本配置，所以通常系统安装完毕后即可在桌面上看到这个“网上邻居”图标。而在 Windows 95/98/XP 等个人操作系统中，安装后可能在桌面上仍会见不到“网上邻居”图标。

2. “网上邻居”中可以看到自己，却看不到其他联网电脑

这可能是“网上邻居”最常见的故障之一了。不过这个故障要比在桌面上没有“网上邻居”图标故障要复杂许多，因为没有“网上邻居”图标属单机问题，而此故障则属于网络互联问题，涉及到许多因素，有常见的软件配置因素，也可能有硬件故障因素。

既然在网上邻居中能够看到自己的计算机，说明本机上的网卡和软件安装均没有问题。但因为所有其他计算机都没有在“网上邻居”中出现，其他计算机同时出现问题的可能性不大，所以出现这种问题的可能性通常是计算机自身和线路故障（包括硬件设备）造成的。可以试着从以下几个方面寻找原因：

（1） 看是否只有一台计算机存在这种问题，还是所有其他计算机都存在这种问题，如果只有个别计算机存在这种问题，则可以肯定的是故障原因基本上与其他计算机无关，只与本机软件配置和相连接的网卡、网线、集线器等设备端口有关。

（2） 确定属于本机或有关的硬件故障有关后，则应分别进行进一步的检测。先排除自身的软件配置问题。

不过在此还要特别提醒各位以下几点：

① 查看所有计算机的 IP 地址是否都配置在同一网段上。

② 是否安装了必须安装的“网络客户端”等选项。

③ 最重要的是要检查在计算机上是否已正确安装启动了“计算机浏览器服务（Computer Browser Service）”。

（3） 如果软件配置没问题，则需要进一步确认硬件部分问题所在。对于这类由硬件造成的故障，当然不能直接把所怀疑的硬件拿去维修，而是要借助于网络软件工具进行测试，以进一步确定是否真是由硬件引起。具体步骤如下：

第 1 步，用 ping.exe 命令 Ping 其他主机的 IP 地址，检查其他计算机的连接速度是否正常，不正常继续进行以下检测操作。如果用 Ping 能 Ping 通，则证明网络硬件连接部分是不存在问题的，很可能问题出在本机软件配置上。

第 2 步，检查网卡状态指示灯是否闪烁，如果闪烁，说明有网络通信数据流量存在，一般可以证明本机与集线器的连接正常。否则应当检查网线的两端是否插好，集线器的电源是否打开。

第 3 步，检查集线器上端口和其他计算机端口的指示灯是否正常。如果正常，说明连网设备与计算机的连接没有问题。否则应当检查网线的两端是否已经插好，并用网线测试仪对网线的连通性重新进行测试，看网线水晶头中的网线芯线是否接触良好。

第 4 步，如果还怀疑其他计算机有软件配置或硬件故障，则可进一步检查。检查其他计算机的网卡灯是否闪烁，如果网卡灯不亮，可能是网卡没有正确安装，也可能是没有和网络连接设备正常连接。在“设备管理器”中检查是否有“网络适配器”选项，或者网络适配器下的设备是否带有“？”或者“！”黄色标记。如果是，表明设备安装不成功，先删除该设备，刷新并重新为其安装驱动程序。如果不是，则证明是网络设备没有问题，或者是网线的问题，按照本文以上检测方法检测其他硬件故障。

1.1.5 局域网互访问题解决经验

关于局域网中不能互访的话题历来都是网管非常关心的，最近提出类似问题的网友也相当多，主要是 Windows98 不能访问 Windows XP，或 Windows2000 不能访问 Windows XP，下面就针对这些互访故障的解决方法做一综述。

1. 使用硬件排除法

用 ping 命令结合看网卡灯的方法可以验证是硬件还是软件方面的原因。先检查网卡灯，如果一个也不亮的话则是网卡有问题。如果只是网卡的信号灯不亮，单击“开始→运行”并输入“ping 对方 IP -t”（实际输入不带引号）如图 1-12 所示。

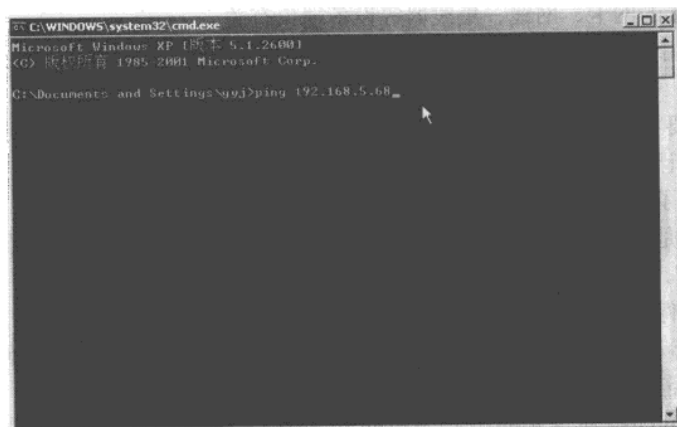


图 1-12 ping 命令

如果提示中连续出现了 4 次“Request timed out”（请求暂停//超时），如图 1-13 所示。

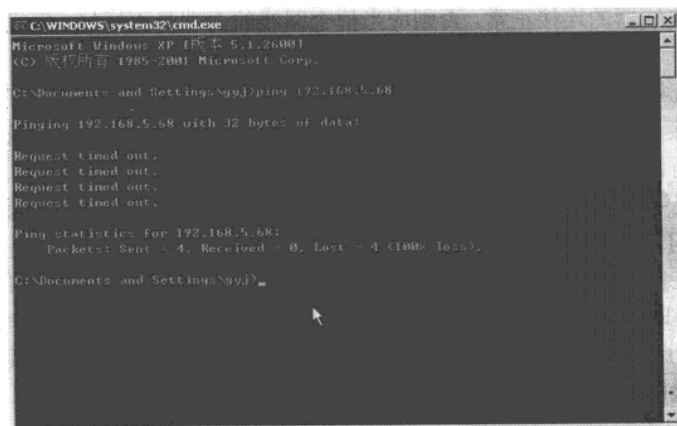


图 1-13 超时

说明物理线路不通或网络太忙造成了阻塞。可用测线仪进一步检查网线及网头，一个一个排除故障。

2. 缺少协议

局域网互访必须的协议：TCP/IP（必要时 IPX/SPX、Novell 网络和某些网络游戏要设定该协议）、NetBIOS。

（1）NetBIOS 协议。

Windows XP 中默认是不支持 NetBIOS 协议的，而现在不少小型网均采用的是该协议，添加方法如下。

第 1 步，复制 Windows XP 安装光盘 Valueadd\MSFT\Net\netbeui 目录下的 nbf.sys 文件到系统的\system32\Drivers 目录中，如图 1-14 所示。

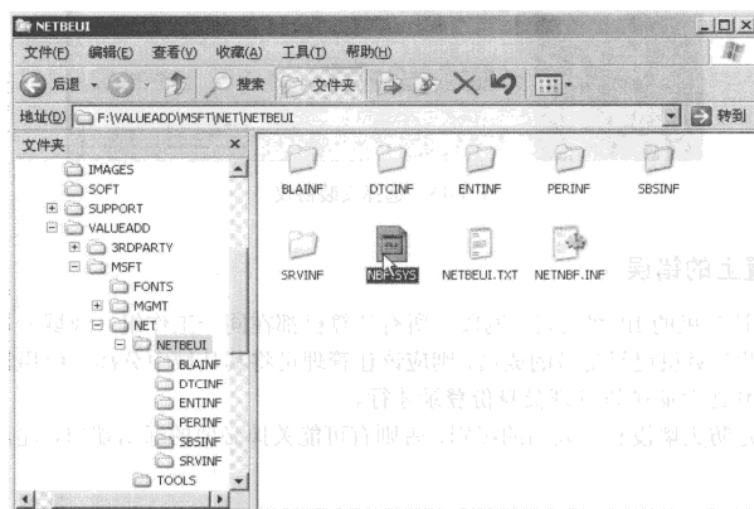


图 1-14 选择复制 nbf.sys 文件

第 2 步，复制 netnbf.inf 到系统的\Inf 目录，然后像通常添加协议那样操作就可以了（在网上邻居有相应添加协议的选项，在光驱中放入 Windows 安装盘直接添加也可以）。

（2）NetBEUI 协议。

该通信协议是 Windows95/98 时代的产物，Windows XP 中已经没有了这类协议（但 NetBEUI 相关文件仍放在 Windows XP 光盘中），有些局域网必须有 NetBEUI 才能存取网络中的某些或全部计算机资料，所以需要动手安装 NetBEUI，方法如下。

放入 Windows XP 安装光盘，到“\VALUEADD\MSFT\NET\NETBEUI”目录下将 Netnbf.inf 复制到 C:\Windows\INF 中；将 Nbf.sys 复制到 C:\Windows\System32\Drivers 中；依次单击“开始→控制面板→网上邻居”，选择“网络连接”图标，在“本地连接”单击鼠标右键，选择“属性”命令，在“常规”选项卡中，依次单击“安装→通讯协议→添加”，此时即可看到“NetBEUI 协议”，选取“NetBEUI 协议”之后，单击“确定”按钮即可，如图 1-15 所示。

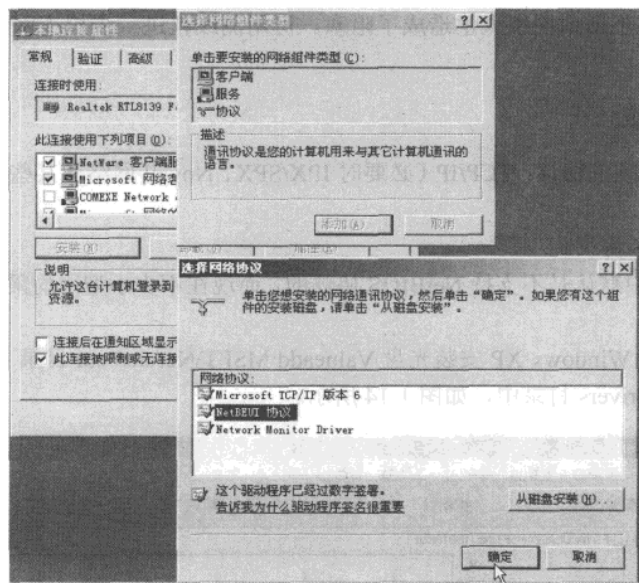


图 1-15 选择安装协议

3. 设置上的错误

确定所有计算机的 IP 都在同一网段，所有计算机都在同一工作组（或域），在更改工作组之前，如果此计算机已经是域的成员，则应该让管理员将其从域中分离并停用该计算机的账户。想修改工作组时必须以管理员身份登录才行。

另外，确定防火墙没有设太高的级别，否则有可能关掉必要的通信端口，建议关掉再试一下。

4. 没有安装服务

要想达到共享的目的，安装“Microsoft 网络文件和打印服务”必不可少，步骤如下。

依次进入“控制面板”→“本地连接”→“属性”→“安装”，在“选择网络组件类型”对话框中单击“服务”→“添加”按钮，在“选择网络服务”对话框中单击要安装的服务即可，如图 1-16 所示。

1.1.6 网络命令全集

读者应该不会忘记 Windows 是从简单的 DOS 字符界面发展过来的，虽然我们平时在使用 Windows 操作系统的时候，主要是对图形界面进行操作，但是 DOS 命令我们仍然非常有用。下面就让我们来看看这些命令到底有那些作用，同时学习如何使用这些命令的技巧。

1. Ping 命令的使用技巧

Ping 是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送

与接收）数据报。根据返回的信息，我们就可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的，我们必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。

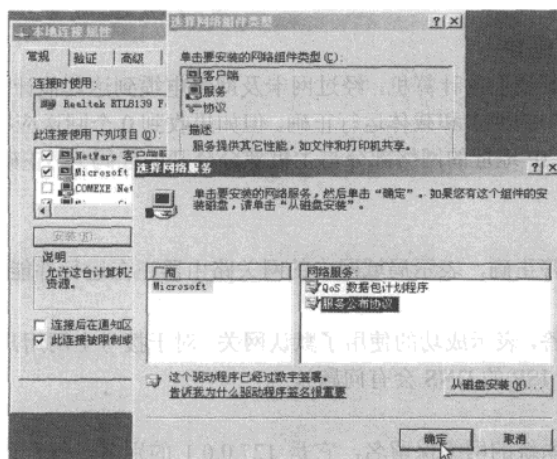


图 1-16 添加服务

简单说，Ping 就是一个测试程序。如果 Ping 运行正确，我们大体上就可以排除网络访问层、网卡、MODEM 的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，Ping 也被某些别有用心的人作为 DDOS（拒绝服务攻击）的工具，例如许多大型的网站就是被黑客利用数百台可以高速接入 Internet 的电脑连续发送大量 Ping 数据报而瘫痪的。

按照默认设置，Windows 上运行的 Ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个 32 字节数据，如果一切正常，我们应能得到 4 个回送应答。Ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。Ping 还能显示 TTL（Time To Live 存在时间）值，我们可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）- 返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段（128-119）；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

（1）通过 Ping 检测网络故障的典型次序。

正常情况下，当我们使用 Ping 命令来查找问题所在或检验网络运行情况时，我们需要使用许多 Ping 命令。如果所有都运行正确，我们就可以相信基本的连通性和配置参数没有问题；如果某些 Ping 命令出现运行故障，它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障。

ping 127.0.0.1。

这个 Ping 命令被送到本地计算机的 IP 软件，该命令永不退出该计算机。如果没有做到这一点，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

网管天下 网管经验谈

ping 本机 IP。

这个命令被送到我们计算机所配置的 IP 地址，我们的计算机始终都应该对该 Ping 命令做出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的 IP 地址。

ping 局域网内其他 IP。

这个命令应该离开我们的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

ping 网关 IP。

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够做出应答。

ping 远程 IP。

如果收到 4 个应答，表示成功的使用了默认网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

ping localhost。

localhost 是操作系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。如果不能实现此功能，则表示主机文件（/Windows/host）中存在问题。

ping www.xxx.com（如 www.baidu.com）。

对这个域名执行 Ping www.xxx.com 地址，通常是通过 DNS 服务器。如果这里出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器了）。顺便说一句：我们也可以利用该命令实现域名对 IP 地址的转换功能。

如果上面所列出的所有 Ping 命令都能正常运行，那么我们对自已的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示我们所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

（2）Ping 命令的常用参数选项。

ping IP -t。

连续对 IP 地址执行 Ping 命令，直到被用户以 Ctrl+C 组合键中断。

ping IP -l 3000。

指定 Ping 命令中的数据长度为 3000 字节，而不是默认的 32 字节。

ping IP -n。

执行特定次数的 Ping 命令。

2. Netstat 命令的使用技巧

Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果我们的计算机有时候接收到的数据报会导致出错数据删除或故障，我们不必感到奇怪，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者它的数目正迅速增加，那么我们就应该使用

Netstat 查一查为什么会出现这些情况了。

(1) Netstat 的一些常用选项。

```
netstat -s
```

本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

```
netstat -e
```

本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。

```
netstat -r
```

本选项可以显示关于路由表的信息类似于后面所讲使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接。

```
netstat -a
```

本选项显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接。

```
netstat -n
```

显示所有已建立的有效连接。
下面是“Netstat”的输出示例，如图 1-17、图 1-18 和图 1-19 所示。

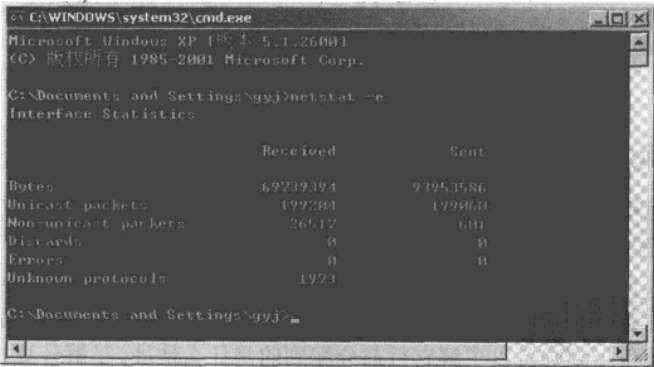


图 1-17 Netstat 输出实例

(2) Netstat 的妙用。

经常上网的人一般都会使用 ICQ，不知道读者是不是曾被一些讨厌的人骚扰，想投诉却又不知从和下手？其实，我们只要知道对方的 IP，就可以向他所属的 ISP 投诉了。但怎样才能通过 ICQ 知道对方的 IP 呢？如果对方在设置 ICQ 时选择了不显示 IP 地址，那我们就无法在信息栏中看到了。其实，我们只要通过 Netstat 就可以很方便的做到这一点。当他通过 ICQ 或

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

其他的工具与我们相连时（例如我们给他发一条 ICQ 信息或他给我们发一条信息），我们立刻在 DOS 命令提示符下输入 netstat -n 或 netstat -a 就可以看到对方上网时所用的 IP 或 ISP 域名了，甚至连所用 Port 都完全暴露了。

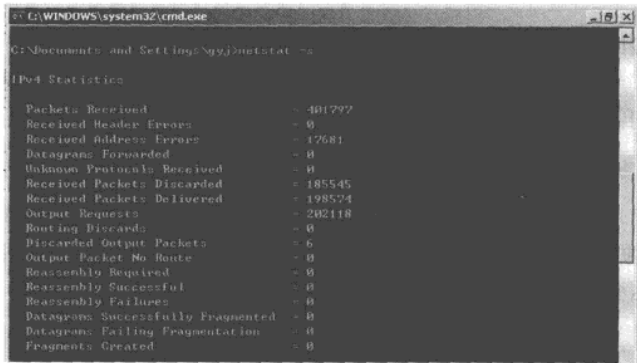


图 1-18 Netstat 输出实例

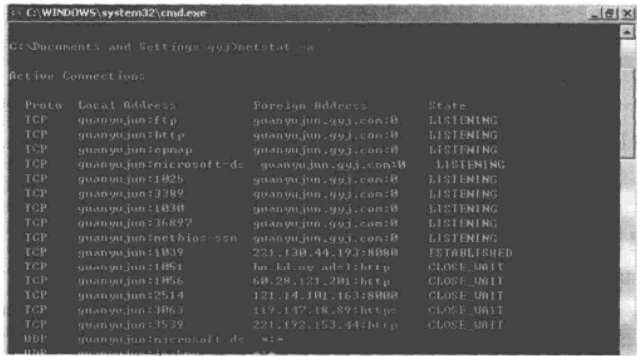


图 1-19 Netstat 输出实例

3. IPConfig 命令的使用技巧

IPConfig 实用程序和它的等价图形用户界面——Windows 95/98 中的 WinIPcfg 可用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。

但是，如果我们的计算机和所在的局域网使用了动态主机配置协议（DHCP），这个程序所显示的信息也许更加实用。这时，IPConfig 可以让我们了解自己的计算机是否成功的租用到一个 IP 地址，如果租用到则可以了解它目前分配到的什么地址。了解计算机当前的 IP 地址、子网掩码和默认网关实际上是进行测试和故障分析的必要项目。

IPConfig 最常用的选项。

Ipconfig

当使用 IPConfig 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和默认网关值。


```
ipconfig /all
```

当使用 all 选项时，IPConfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，IPConfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

```
ipconfig /release  
ipconfig /renew
```

这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果我们输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。请注意，大多数情况下网卡将被重新赋予和以前相同的 IP 地址。

■ 4. ARP（地址转换协议）的使用技巧

ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。使用 arp 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理/IP 地址对，我们可能会使用这种方式为默认网关和本地服务器等常用主机进行修复，有助于减少网络上的信息量。

按照默认设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使用，物理/IP 地址对就会在 2~10 min 内失效。因此，如果 ARP 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 arp 命令查看高速缓存中的内容时，请最好先 ping 此台计算机（不能是本机发送 ping 命令）。

ARP 常用命令选项。

```
arp -a 或 arp -g
```

用于查看高速缓存中的所有项目。-a 和 -g 参数的结果是一样的，多年来 -g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的 -g 选项。

```
arp -a IP
```

如果我们有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

```
arp -s IP
```

我们可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

```
arp -d IP
```

使用本命令能够人工删除一个静态项目。

例如我们在命令提示符下，输入 arp -a；如果我们使用过 Ping 命令测试并验证从这台计

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

算机到 IP 地址为 202.206.197.65 的主机的连通性，则 ARP 缓存显示如图 1-20 所示。

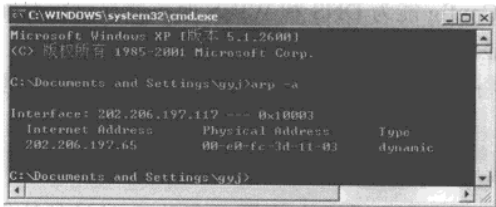


图 1-20 显示 ARP 缓存

1.2 轻松上网的经验

本节重点介绍了上网过程中出现的一些基本故障的解决，例如怎样保证计算机能与 Internet 保持接通状态，在连接不上网络的时候该如何解决等。

1.2.1 快速修复 Windows Vista 不能连接网络的小经验

用过 Windows Vista 的人都知道，Windows Vista 有时候会出现连接网络失败，这种情况通常是由于一些老式的路由器并不总是严格遵循标准造成的。本节介绍的就是遇到类似问题的解决方法。

首先你要用管理员用户身份登录，然后依次按照本节叙述操作即可。

第 1 步，单击“开始”→“附件”，选择并右击“命令提示符”从弹出的菜单中选择“以管理员身份运行”命令行如图 1-21 所示，实现以管理员身份运行命令行。

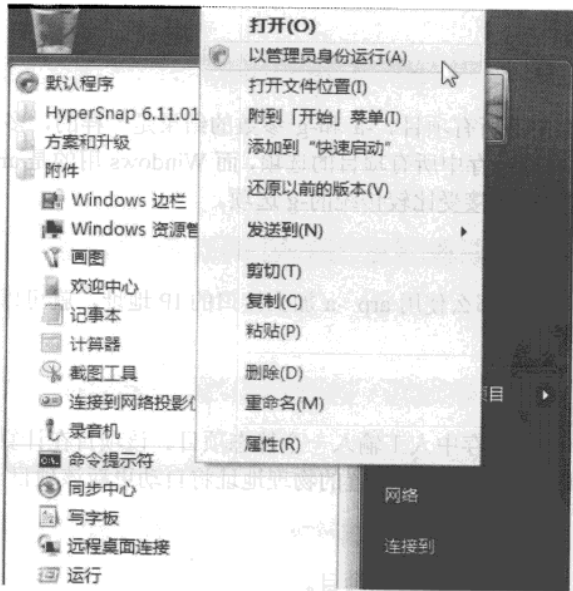


图 1-21 以管理员身份运行命令行

第 2 步，在命令行中输入命令“C:\Windows\system32>netsh interface tcp show global”如图 1-22 所示，实现查看当前的 TCP 优化设置的功能。



图 1-22 查看 TCP 优化设置

第 3 步，我们会在控制台中收到一个类似于如图 1-23 所示的回复信息。



图 1-23 TCP 全局参数

第 4 步，在命令行执行“C:\Windows\system32>netsh interface tcp set global rss=disabled autotuninglevel=disabled”，如图 1-24 所示，实现禁用第 3 步中所查到的一些设置的功能。

第 5 步，在命令提示行中收到如图 1-25 所示的回复。

此时尝试连接一下网络，如果不行，因为一般用户使用的是有线网络，可能需要“修复”一下网络连接或者对网络电缆进行拔插后再重新连接，这样问题应该就会得到解决。如果使用的是无线网络，只需断开网络然后再连接到网络问题便会得到解决。

第 6 步，如果问题仍没能解决，可以在命令行输入“C:\Windows\system32>netsh interface tcp set global rss=enabled autotuninglevel=normal”如图 1-26 所示，实现将网络栈等设置回正常的状态。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

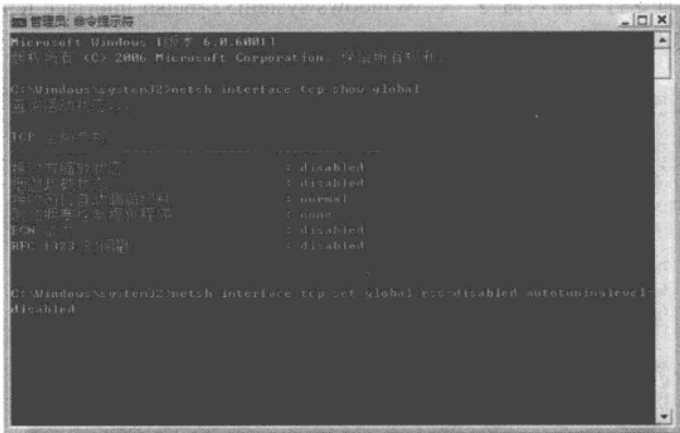


图 1-24 禁止 TCP 的一些功能

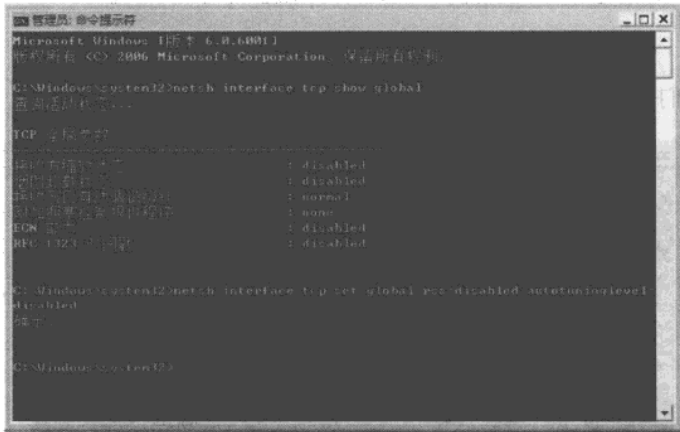


图 1-25 禁用成功



图 1-26 恢复 TCP 设置

说
·
明

Windows Vista 可以调整其网络设置，以最大程度的利用可用的网络带宽。

1.2.2 解决网络故障的方法总结

其实许多网络故障，自己通过努力都是可以解决的，只是有时缺少解决问题的思路与方法。只要掌握了这些思路与方法，你就能做到一般网络故障不求人了。解决问题的方法有许多，而每个人解决问题的思路也不一样。在本节作者将以个人的经验为例，介绍解决网络故障的方法与思路，希望能对读者有所启发和帮助。

首先在解决网络故障之前，需要了解整个网络的拓扑，要知道网络中有那些设备，这些设备之间是怎样连接的。如果是局域网内的设备，需要知道各个设备的 IP 地址、子网掩码，如果是广域网设备或者是连接到 Internet，需要了解 IP 地址、子网掩码、网关地址、DNS 地址和路由表信息。最好的情况是有一张详细的网络拓扑图，根据拓扑图分析。

然后你应该像熟悉从单位回家的路一样，熟悉网络中的设备以及网络拓扑情况。如果你详细了解每条回家的路，在某些情况下，例如下大雨的时候，你可以根据以前的经验判断，回家途中的哪个地道可能会由于雨水过大而不能通行，这样你就可以选择另一条路顺利地回到家。

同样如果你熟悉你所在城市的每一条路，当你的朋友打电话向你问路时，在了解他所处的位置后，你会告诉他从当前位置向那个方向走，过几个路口，乘几路车，坐几站换乘几路车就可以到达目的地。而解决网络中的故障是和“指路”差不多的相同性质的工作。

总体来说，如果按照用户划分，网络故障可以分为“企业中的”网络故障与“个人用户”网络故障。对于企业中的网络故障来说，如果按照产品功能划分，通常包括“工作站故障”、“服务器故障”、“网络设备故障”、“线路故障”与“其他故障”，下面分别进行介绍。

在解决此类故障时，应本着“从简单到复杂”、“从软件故障到硬件故障”的原则进行判断。根据故障出现在工作环境中的地位的不同，我们将其大致分为以下几个部分来具体讨论。

1. 工作站故障

对于工作站故障，通常来说，采用“代替法”与“排除法”即可以解决。当网络中的工作站出现问题时，首先要清楚，是网络中的所有工作站都出现了问题，还是某一组中的工作站出现问题，或者仅仅是某一台工作站出了问题。

如果网络中的所有工作站都出现了同一个问题，例如，都不能登录服务器，或者登录服务器很慢，或者都不能访问某些网站。这时候的故障，应该在工作站到故障点之间的线路或者某些设备上，例如，核心交换机出现问题、所有用过 Windows Vista 的人都知道，Windows Vista 有时候会出现连接网络失败，这种情况通常是由于一些老式的路由器并不总是严格遵循标准造成的。本节介绍的就是遇到类似问题的解决方法。

工作站的上级交换机或者路由器或者服务器出现问题，甚至是网络的出口（广域网或者 Internet 网络）出现问题。这时候，可以在网络中的任意一台工作站上，使用 ping 命令，依次

网管天下 网管经验谈

检查到上一级设备的连接情况，逐级检查以定位故障点，最后排除故障。

例如，对于类似于图 1-27 所示的网络拓扑情况，当所有的工作站不能访问服务器 Server 或者不能访问 Internet 时，可以在网络中的任意一台工作站上（例如 W1），使用 ping 命令，首先检查到 S3 交换机的连通性。如果到 S3 不能连通，则检查 S3 交换机的配置情况，在确认不是配置问题后，检查 S3 交换机是否损坏，如果 S3 交换机损坏，根据情况维修或者更换。

然后检查到服务器的连通性，如果不能访问服务器，就检查 S3 与服务器之间的线路，之后依次检查服务器的网卡、服务器的配置。对于 S3 与服务器之间的线路，可以用“代替法”进行检查，就是找一段好的线路代替 S3 与服务器原来的连线，检查是否该线路问题。在排除线路问题后，可以确认是服务器出现了问题（关于服务器问题的解决请看后文“服务器故障”一节）。如果不能访问 Internet，则需要依次检查 S3 到路由器（或代理服务器、防火墙）之间的线路、路由器的配置、路由器到 Internet 的线路情况，然后再检查是否存在 ISP 的故障等。实际上，如果网络中的所有工作站都不能访问外网，则首先要在代理服务器或者路由器上，检查连接到上级的线路是否正常，在排除上级线路（ISP）的故障后，检查 S3 与路由器之间的线路、路由器的配置等情况。

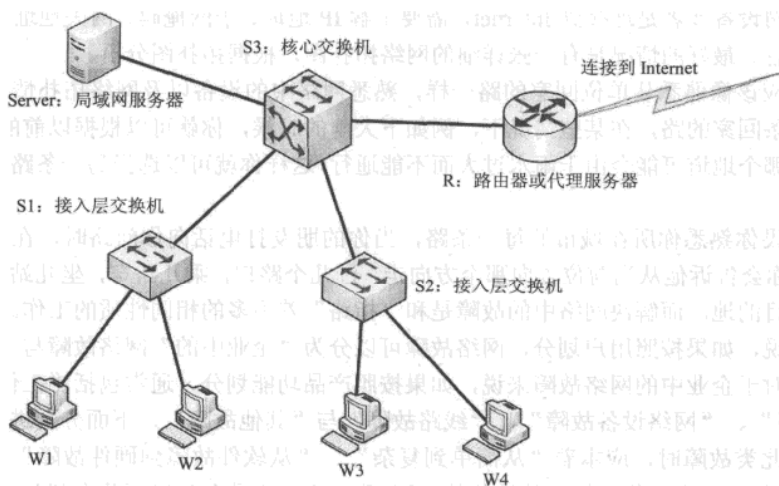


图 1-27 网络拓扑图

如果网络中的某些工作站出现问题，而网络中的其他组都正常时，要检查出现问题的工作站与其他组能否互通。例如，对于图 1-27 来说，如果 S2 中的工作站都不能访问服务器或者不能访问 Internet，则首先要检查 S2 中的工作站能否与 S1 中的工作站互通（最简单的是使用 ping 命令检查），如果 S2 与 S1 能互通，则表明 S2 中的工作站不能访问服务器或者 Internet，是服务器与路由器的设置问题造成的；如果 S2 中的工作站与 S1 中的服务器不能互通，则表明是 S2 交换机、S2 与 S3 的连线或者 S3 交换机的设置引起的。这时候，按照顺序依次检查并排除即可。

如果网络中的一台工作站出现问题，例如，W3 不能访问服务器（或 Internet），而网络中其他的工作站都正常，可以按照如下的步骤解决：

第 1 步，在 W3 工作站上，使用 ping 命令，检查是否可以 ping 通 W4 或 S2 或 S3 交换机，

如果能 ping 通这些工作站或交换机，则表示 W3 不能访问服务器（或 Internet）是服务器端对 W3 进行了限制。如果不能 ping 通，则进行下面的检查。

第 2 步，打开“网络连接”，查看是否出现图 1-28 所示的“网络电缆被拔出”的连接，如果出现这种问题，表明是网线问题，或者是连接 W3 的 S2 交换机端口出现问题。

第 3 步，打开“网络连接”，用鼠标右键单击“本地连接”，是否出现“启用”端口，如果出现，表示当前网卡被禁用，启用网卡即可，如图 1-29 所示。



图 1-28 网线没有接好

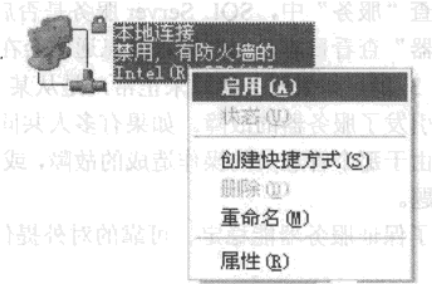


图 1-29 网卡被禁用

第 4 步，之后检查网卡配置是否正确（IP 地址、子网掩码、网关地址），如果是通过 DHCP 方式获得地址，检查是否获得地址，如果获得的地址是 0.0.0.0 或 169.254.x.x，则表示 IP 地址没有获得；如果获得的地址的子网掩码为 0.0.0.0，则表示 IP 地址冲突。在这些情况下，可以“手动”指定网络中正确的地址。在确认不是 IP 地址或者配置的情况后，查看 W3 网卡的状态（如图 1-30 所示），如果“状态”只有发送数据，而没有收到数据时，表示是 W3 的网卡或者是 W3 的网线或 S2 交换机上连接 W3 的端口出现问题，

如果出现这种情况，可以将连接 W4 的网线插到 W3 上（当 W4 与 W3 离的很近时），检查线路是否问题，如果 W4 与 W3 很远，可以用测线仪检查 W4 网线是否有故障。如果网线没有故障，则可以在 S2 上，将连接 W4 的网络更换一下端口，在排除交换机端口与网线故障后，那就是 W3 这台工作站的问题了。这时候，可以“禁用”W3 的网卡，然后再启用，如果不能解决，可以在“设备管理器”中，卸载 W3 的网卡，然后重新启动计算机，进入系统后重新安装网卡驱动程序。如果问题仍然没有解决，可以尝试为 W3 更换一块网卡，如果问题仍然不能解决，只能重新安装操作系统了。

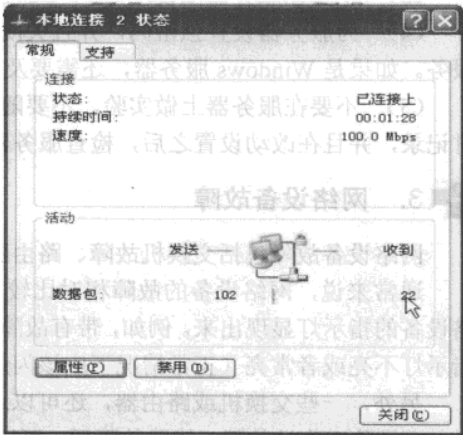


图 1-30 查看状态

2. 服务器故障

服务器故障主要包括硬件故障、软件故障与操作系统故障等。当网络中的服务器出现故障时，可以依据下面的顺序进行检查：

网管天下 网管经验谈

第 1 步，检查外观：服务器能否启动，如果服务器已经处于登录状态，不要着急重新启动服务器，先检查服务器的指示灯，例如电源、硬盘指示灯，或者其他警报指示灯。当指示灯正常时，可以登录到控制台，使用 ping 命令，检查服务器的网络连通性。如果不能连通，检查服务器 TCP/IP 设置、网卡驱动程序、网卡、网线等问题。

第 2 步，当网络连通时，检查所提供的“服务”是否启动，工作是否正常。如果这台服务器是 SQL Server 服务器，就要登录“SQL Server 企业管理器”，查看服务状态是否正常，或者检查“服务”中，SQL Server 服务是否启动。如果是 Windows 服务器，还可以使用“事件查看器”查看日志，一些错误信息通常会在日志中反应出来。

第 3 步，如果服务器原来正常，是从某个时间或者某个操作后不正常，则检查相关的操作是否引发了服务器的故障。如果有多人共同管理服务器，就请所有管理服务器的人到一起，询问是由于那个管理员的操作造成的故障，或者检查上次管理人员对服务器的操作记录，从而解决问题。

为了保证服务器能稳定、可靠的对外提供服务，通常来说，管理服务器需要做到以下几点：

- (1) 保证服务器所在机房的温度、湿度在规定范围内，并且不要让机房有太多的灰尘。
- (2) 保证机房的供电电压稳定。
- (3) 不要在服务器上使用 QQ、BT 等软件，也不要服务器上测试软件。
- (4) 为服务器设置强密码，并且关闭服务器不使用的端口，禁用或停用服务器不需要的服务。如果是 Windows 服务器，还需要及时更新补丁。
- (5) 不要在服务器上做实验，不要随意改动服务器的设置。如果改动了设置，一定要及时记录，并且在改动设置之后，检查服务器能否正常工作。

3. 网络设备故障

网络设备故障包括交换机故障、路由器故障、光纤收发器等设备不能正常工作时的状态。

通常来说，网络设备的故障相对比较好定位或排除。当网络设备出问题后，通常能从网络设备的指示灯显现出来。例如，带有故障显示的高端路由器、交换机，或者是普通的交换机，指示灯不亮或者常亮（正常情况下应该闪烁而不是一直亮），这些都很容易区分。

另外，一些交换机或路由器，还可以通过 telnet 或 Web 方式管理，当不能登录这些设备时，在排除工作站故障、线路故障后，可以定位到设备故障。一些可管理的交换机，还可以通过控制线进行设置，当使用控制线不能登录时（排除设置工作站与控制线问题后），可以判断是交换机问题。

4. 线路故障

线路指的是连接工作站（或服务器）与网络设备之间的线路，例如工作站到交换机的 RJ45 网线，服务器到核心交换机的光纤（或 RJ45 网线），交换机与交换机（或路由器、网关、防火墙或代理服务器等）之间的 RJ45 网线或光纤等，线路还包括到 ISP 的接线，例如光纤或 DDN、ADSL 线路等。

如果怀疑 RJ45 网线故障，可以用测线仪检查，或者通过其他已证明完好的网线代替来检查，如果是光纤，可以看连接光纤设备的指示灯，或者用测光纤的设备检查。如果是到 ISP 的线路，可以请 ISP 工作人员检查。

5. 个人用户网络故障

个人用户网络故障，指的是个人或家庭用户，通过 ADSL、电话拨号或者小区提供的入户网线提供的宽带网络连接所出现的故障。如果是几家共用路由器、ADSL 共享上网，则可以按照前面“工作站故障”等内容解决。这里只介绍一家直接上网问题的故障解决。

如果是个人用户网络故障，通常来说，也就是宽带拨号故障、ADSL 接计算机网线故障、计算机故障几部分。如果是宽带拨号故障，可以检查 ADSL 的指示灯，然后查看是到 ISP 的宽带线路故障，还是用户名、密码故障，这些在拨号的时候会有显示。如果是网线或计算机故障，可以参见本节第一部分中的相关内容。

1.2.3 解决网络变慢的经验

局域网中众多计算机出现问题而不能使用，整个网络速度在上班高峰时间非常缓慢。以上所说的情况想必不止一个人遇到过，大部分网管员都会为之烦恼。所以在这里我把自己的一些见解和经验同大家分享。其实造成网络变慢的原因不外乎以下几种情况：

（1）由于大多数客户机安装的是 Windows 操作系统，而员工没有及时更新 Windows 操作系统的补丁，导致计算机系统存在多个漏洞。员工在浏览一些网站时，感染了针对某个漏洞的木马或病毒，这些木马或病毒会尝试扫描并攻击网络中其他计算机。另外，木马或病毒还会尝试在后台浏览广告网站或者下载一些病毒程序，这些都会占用大量的网络带宽。

（2）现在大多数单位都安装了杀毒软件，但许多员工没有及时更新病毒库，或者虽然更新了病毒库，但当感染病毒时不会清除。

（3）某些员工习惯于浏览一些网站，或者经常下载一些软件或电影，而现在提供软件或电影下载的网站，为了自身的利益，都会捆绑一些流氓软件或者木马程序，有的软件还带有病毒。

（4）现在许多计算机感染了 ARP 病毒，这也是网络缓慢的一个原因。

（5）由于一些单位没有划分 VLAN，所以当单位中一台计算机感染病毒并扫描整个网络或者对整个网络的计算机进行攻击时，就会导致整个网络瘫痪。

找到问题的根源后，就需要针对以上问题逐步进行解决：

第 1 步，划分 VLAN 必不可少。虽然很多企业也有三层交换机，但是并没有划分 VLAN。没有划分 VLAN 的原因很多，一个最主要的原因就是遗留问题。刚开始的时候，企业中计算机数量比较少，没有划分的必要。当单位的计算机数量增加到 80 台以上的时候，就要考虑划分 VLAN。划分 VLAN 后，可以屏蔽 VLAN 之间的广播，当网络中的计算机出现问题导致对外广播大量数据包的时候，只会影响自己的 VLAN（当然，如果每个 VLAN 中都有大量广播数据包的计算机，也会影响整个网络）。

划分 VLAN 至少需要一个三层交换机。在划分的时候，可以按照楼层或者按照部门的原则划分。如果网络中没有三层交换机，而单位中计算机数量又不是非常多的时候，可以在 Windows 2000 Server 或者 Windows Server 2003 的计算机上，安装多块网卡。每个网卡连接一台交换机，使用 Windows Server 2003 的软路由划分 VLAN，可以完成三层交换机的功能。

划分 VLAN 后，还要将单位中每台计算机（尤其是服务器）的 MAC 地址与 IP 地址绑定。在这方面，政府部门做的最好，几乎所有的政府部门，计算机的 MAC 地址与 IP 地址都进行

网管天下 网管经验谈

了绑定。但许多机关、事业单位、学校的网络没有绑定，这就导致现在 ARP 病毒爆发时，单位的网络速度奇慢。

第2步，自动升级更安全更可靠。单位工作站操作系统大多是 Windows XP、Windows 2000、Vista，办公软件用 Office，上网用 IE。如果这些系统或软件没有及时更新 Microsoft 发布的最新补丁，在网上网的时候就可能遭受攻击或者感染木马、病毒程序。即使计算机不上网，如果单位中其他计算机感染了病毒或木马，也会被感染。

在企业网络中采用 Microsoft 的 WSUS 服务器，可以很好地解决这个问题。WSUS 当前版本是 3.0，可以为 Windows 2000、Windows XP、Windows Server 2003、Windows Vista、IE6、IE7、Office 2003、Office XP、Office 2007、SQL Server 等产品提供补丁程序。WSUS 的安装与配置本文不做过多介绍，只是要注意以下几个问题：① 在 WSUS 第一次安装好之后，首先要从 Microsoft 网站进行更新，更新之后，要手动审批补丁之后，补丁文件才会下载。② 在补丁下载完成后，修改 WSUS 的选项，并创建自动审批、自动下载选项，以后 WSUS 可以不经管理员手动审批即可以自动从 Microsoft 网站下载补丁到 WSUS 服务器。③ 工作站配置好后，可以进入命令提示符，使用 `wuauclt/detectnow` 或 `wuauclt1/detectnow` 命令，立刻与局域网内的 WSUS 进行同步，并且可以使用 `netstat an` 命令检查到 WSUS 服务器的连接，如果与 WSUS 服务器连接正常，应该有到服务器 IP 地址与端口的连接信息。

大多数杀毒软件，例如卡巴斯基、NOD32、金山毒霸等，都提供了局域网升级功能，只要在网络中找一台计算机做服务器，这台服务器从厂商的网站升级，并把病毒库作为共享文件夹，网络中其他工作站都可以从共享文件夹或该 Web 服务器升级。只要及时升级病毒库并开始文件实时防毒功能，一般情况下，都能对计算机进行很好的防护。

第3步，精选工具做到全面监控。大多数单位上网，都是用的路由器的 NAT 功能，也有的单位购买硬件防火墙。硬件防火墙配置复杂、更改配置不易，不易增加垃圾网站或者有问题网站的禁止访问列表，而路由器中的 NAT 就没有这项功能。此时，可以用好的软件防火墙，例如 Microsoft 的 ISA Server 代替原来的路由器或硬件防火墙，改进网络出口的管理。使用 ISA Server 的时候，如果启用“入侵检测”后，外网对 ISA Server 的扫描、入侵都会被 ISA Server 拒绝并记录对方的 IP 地址，在启用“定义连接限制”后，可以限制内网中每个 IP 地址每分钟最大的并发连接数。当达到或超过限制后，在 ISA Server 上会记录该 IP 地址并限制该 IP 进行新的连接。这样，当单位中的计算机感染木马或病毒，试图在网上广播时，会在第一时间被 ISA Server 记录。同时，如果内网中的计算机使用 BT、Flashget 等多线程或 P2P 工具下载软件时，达到限制的并发连接数也会被 ISA Server 记录。管理员可以通过 ISA Server 的监视记录查看入侵或超过限制的计算机的 IP 地址。

在本节介绍的方案指导下，近两年来给多个政府、企业、学校进行了网络升级改造，从这些单位最近两年的使用情况来看，效果非常好。但在使用过程中，也需要注意某些问题。如保存 WSUS 升级补丁的硬盘一定要有足够的空间。另外，服务器硬盘相对来说都比较小。在这种情况下，如果我们给服务器增加新的硬盘，要使用 Windows Server 2003 的动态卷功能，把 WSUS 补丁所在分区转换成动态卷，并且把新安装的硬盘转换成动态卷，扩展保存 WSUS 补丁所在的硬盘分区，增加硬盘的可用空间，然后重新从 Microsoft 网站同步并下载补丁。

1.3 路由器故障解决经验

本节只介绍了两个方面的内容：一方面是关于路由器、交换机、集线器等设备的一些基本常识。另一方面介绍了由于路由器的原因所引起的网络故障的排除方法和经验。

1.3.1 交换机、路由器、集线器、网卡等网络设备的区别和联系

网卡和路由器是两种网络硬件设备。网卡是网络终端与网络的接口设备；而路由器是用来引导网络中的信息传输的。

（1）集线器。

集线器实际就是一种多端口的中继器。集线器一般有(4)(8)1(6)2(4)32等数量的RJ45接口，通过这些接口，集线器便能为相应数量的计算机完成“中继”功能（将已经衰减得不完整的信号经过整理，重新产生出完整的信号再继续传送）。由于它在网络中处于一种“中心”位置，因此集线器也叫做“Hub”。

集线器的工作原理很简单，比如有一个具备8个端口的集线器，共连接了8台计算机。集线器处于网络的“中心”，通过集线器对信号进行转发；8台计算机之间可以互通。具体通信过程是这样的：假如计算机1要将一条信息发送给计算机8，当计算机1的网卡将信息通过双绞线送到集线器上时，集线器并不会直接将信息送给计算机8，它会将信息进行“广播”——将信息同时发送给8个端口，当8个端口上的计算机接收到这条广播信息时，会对信息进行检查，如果发现该信息是发给自己的，则接收，否则不予理睬。由于该信息是计算机1发给计算机8的，因此最终计算机8会接收该信息，而其他7台计算机看完信息后，会因为信息不是自己的而不接收该信息。

（2）交换机。

交换机也叫交换式集线器，它通过对信息进行重新生成，并经过内部处理后转发至指定端口，具备自动寻址能力和交换作用，由于交换机根据所传递信息包的目的地址，将每一信息包独立地从源端口送至目的端口，避免了和其他端口发生碰撞。广义的交换机就是一种在通信系统中完成信息交换功能的设备。

在计算机网络系统中，交换机是针对共享工作模式的弱点而推出的。集线器是采用共享工作模式的代表，如果把集线器比作一个邮递员，那么这个邮递员是个不认识字的“傻瓜”——要他去送信，他不知道直接根据信件上的地址将信件送给收信人，只会拿着信分发给所有的人，然后让接收的人根据地址信息来判断是不是自己的！而交换机则是一个“聪明”的邮递员——交换机拥有一条高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背部总线上，当控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的MAC（网卡的硬件地址）的NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口。目的MAC若不存在，交换机才广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部地址表中。

可见，交换机在收到某个网卡发过来的“信件”时，会根据上面的地址信息，以及自己掌握的“常住居民户口簿”快速将信件送到收信人的手中。万一收信人的地址不在“户口簿”上，交换机才会像集线器一样将信分发给所有的人，然后从中找到收信人。而找到收信人之后，交

网管天下 网管经验谈

换机会立刻将这个人的信息登记到“户口簿”上，这样以后再为该客户服务时，就可以迅速将信件送达了。

（3）路由器。

路由器是网络中进行网间连接的关键设备。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互连网络 Internet 的主体脉络。

路由器之所以在互联网中处于关键地位，是因为它处于网络层，一方面能够跨越不同的物理网络类型（DDN、FDDI、以太网等等），另一方面在逻辑上将整个互连网络分割成逻辑上独立的网络单位，使网络具有一定的逻辑结构。路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。

路由器的基本功能是，把数据（IP 报文）传送到正确的网络，细分则包括：① IP 数据报的转发，包括数据报的寻径和传送；② 子网隔离，抑制广播风暴；③ 维护路由表，并与其他路由器交换路由信息，这是 IP 报文转发的基础；④ IP 数据报的差错处理及简单的拥塞控制；⑤ 实现对 IP 数据报的过滤和记账。

路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的性能则直接影响着网络互连的质量。因此 Internet 研究领域，路由器技术始终处于核心地位。

交换机、集线器、路由器到底有何区别和联系呢？

首先说 HUB，也就是集线器。它的作用可以简单的理解为将一些计算机连接起来组成一个局域网。而交换机（又名交换式集线器）作用与集线器大体相同。但是两者在性能上有区别：集线器采用的是共享带宽的工作方式，而交换机是独享带宽。这样在计算机很多或数据量很大时，两者将会有比较明显的不同。

路由器与以上两者有明显区别，它的作用在于连接不同的网段并且找到网络中数据传输最合适的路径，可以说一般情况下个人用户需求不大。路由器是产生于交换机之后，就像交换机产生于集线器之后一样，所以路由器与交换机也有一定联系，并不是完全独立的两种设备。路由器主要克服了交换机不能转发数据包的不足。

总的来说，路由器与交换机的主要区别体现在以下几个方面：

（1）工作层次不同。

最初的交换机是工作在 OSI / RM 开放体系结构的数据链路层，也就是第二层，而路由器一开始就设计工作在 OSI 模型的网络层。由于交换机工作在 OSI 的第二层（数据链路层），所以它的工作原理比较简单，而路由器工作在 OSI 的第三层（网络层），可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

（2）数据转发所依据的对象不同。

交换机是利用物理地址或者说 MAC 地址来确定转发数据的目的地址。而路由器则是利用不同网络的 ID 号（即 IP 地址）来确定数据转发的地址。IP 地址是在软件中实现的，描述的是设备所在的网络，有时这些第三层的地址也称为协议地址或者网络地址。MAC 地址通常是硬件自带的，由网卡生产商来分配的，而且已经固化到了网卡中去，一般来说是不可更改的。而 IP 地址则通常由网络管理员或系统自动分配。

（3）传统的交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域。

由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第三层以上交换机具有 VLAN 功能，也可以分割广播域，

但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

（4）路由器提供了防火墙的服务。

路由器仅仅转发特定地址的数据包，不传送不支持路由协议的数据包传送和未知目标网络数据包的传送，从而可以防止广播风暴。

交换机一般用于 LAN-WAN 的连接，交换机归于网桥，是数据链路层的设备，有些交换机也可实现第三层的交换。路由器用于 WAN-WAN 之间的连接，可以解决异性网络之间转发分组，作用于网络层。他们只是从一条线路上接受输入分组，然后向另一条线路转发。这两条线路可能分属于不同的网络，并采用不同协议。相比较而言，路由器的功能较交换机要强大，但速度相对也慢，价格昂贵，第三层交换机既有交换机线速转发报文能力，又有路由器良好的控制功能，因此得以广泛应用。

目前个人使用比较多的宽带接入方式就是 ADSL，因此作者就 ADSL 的接入来简单的说明一下。现在购买的 ADSL 猫大多具有路由功能（很多的时候厂家在出厂时将路由功能屏蔽了，因为电信安装时大多是不启用路由功能的，所以需要手动启用 DHCP 并打开 ADSL 的路由功能），如果个人上网或少数几台通过 ADSL 本身就可以了，如果计算机比较多你只需要再购买一个或多个集线器或者交换机。考虑到如今集线器与交换机的价格相差十分小，不是特殊的原因，请购买一个交换机。不必去追求高价，因为如今产品同质化十分严重，我买的最便宜的交换机使用到现在也没有任何问题。给你一个参考报价，建议你购买一个 8 口的，以满足扩充需求，一般的价格在 100 元左右。接上交换机，所有计算机再接到交换机上就行了。余下所要做的事情就只有把各个计算机的网线插入交换机的接口，将 ADSL 的网线插入 uplink 接口。然后设置路由功能，DHCP 等，就可以共享上网了。

看完以上的介绍，相信读者应该对交换机、集线器、路由器已经有了一些了解，目前主要还是以交换机、路由器的组合使用为主，具体的组合方式可根据具体的网络情况和需求来确定。

1.3.2 路由引起的网络故障排除经验

前面 1.2.2 节讲了一些网络故障的解决经验总结，一般的计算机方面的故障相对好解决，但是当遇到的网络故障时由路由器引起的，似乎就不是大家熟悉的了。所以本节就是总结一下由路由器引起的网络故障的排除经验。网络故障的诊断，不管是哪方面引起的，其原理及排除故障的思路是一样的。从故障现象出发，根据经验来着手查找故障点，找出故障原因，排除故障从而使网络能正常通信。

网络故障通常有以下几种可能：物理层中物理设备相互连接失败或者硬件及线路本身的问题；数据链路层的网络设备的接口配置有问题；网络层网络协议配置或操作错误；传输层的设备性能或通信拥塞问题；上三层或网络应用程序错误。

网络诊断可以使用工具：路由器诊断命令，网查看路由表，是开始查找网络故障的好办法。ICMP 的 ping、trace 命令和 Cisco 的 show 命令、debug 命令是获取故障诊断有用信息的网络工具。如利用 show interface 命令可以获得待检查的每个接口的信息。show buffer 命令提供定期显示缓冲区大小、用途及使用状况。show proc 命令和 show proc mem 命令可用于跟踪处理器和内存的使用情况。可以定期收集这些数据，在故障出现时用于诊断参考。

1. 根据网络分层来一步步排除由路由引起的网络故障

(1) 物理层的故障主要表现在设备的物理连接方式是否恰当；连接电缆是否正确；Modem、CSU/DSU 等设备的配置及操作是否正确。确定路由器端口物理连接是否完好的最佳方法是使用 `show interface` 命令，检查每个端口的状态，通过屏幕输出信息，查看端口状态、协议建立状态和 EIA 状态。

(2) 数据链路层的故障，需要查看路由器的配置，检查连接端口的共享同一数据链路层的封装情况。每对接口要和与其通信的其他设备有相同的封装。通过查看路由器的配置检查其封装，或者使用 `show` 命令查看相应接口的封装情况。

(3) 排除网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由。然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障，包括 RIP 或者 IGRP 路由协议出现的故障。例如，对于 IGRP 路由，选择信息只在同一自治系统号（AS）的系统之间交换数据，查看路由器配置的自治系统号的匹配情况。

2. 路由器接口故障排除

(1) 串口故障排除：串口出现连通性问题时，为了排除串口故障，一般是从 `show interface serial` 命令开始，分析它的屏幕输出报告内容，找出问题之所在。串口报告的开始提供了该接口状态和线路协议状态。接口和线路协议的可能组合有以下几种：

① 串口运行、线路协议运行，这是完全的工作条件。该串口和线路协议已经初始化，并正在交换协议的存活信息。

② 串口运行、线路协议关闭，这个显示说明路由器与提供载波检测信号的设备连接，表明载波信号出现在本地和远程的调制解调器之间，但没有正确交换连接两端的协议存活信息。可能的故障发生在路由器配置问题、调制解调器操作问题、租用线路干扰或远程路由器故障，数字式调制解调器的时钟问题，通过链路连接的两个串口不在同一子网上，都会出现这个报告。

③ 串口和线路协议都关闭，可能是电信部门的线路故障、电缆故障或者是调制解调器故障。

④ 串口管理性关闭和线路协议关闭，这种情况是在接口配置中输入了 `shutdown` 命令。通过输入 `no shutdown` 命令，打开管理性关闭。

在接口和线路协议都运行的状况下，虽然串口链路的基本通信建立起来了，但仍然可能由于信息包丢失和信息包错误出现许多潜在的故障问题。正常通信时接口输入或输出信息包不应该丢失，或者丢失的量非常小，而且不会增加。如果信息包丢失有规律性增加，表明通过该接口传输的通信量超过接口所能处理的通信量。解决的办法是增加线路容量。查找其他原因发生的信息包丢失，查看 `show interface serial` 命令的输出报告中的输入输出保持队列的状态。当发现保持队列中信息包数量达到了信息的最大允许值，可以增加保持队列设置的大小。

(2) 以太接口故障排除：以太接口的典型故障问题是，带宽的过分利用；碰撞冲突次数频繁；使用不兼容的帧类型。使用 `show interface ethernet` 命令可以查看该接口的吞吐量、碰撞冲突、信息包丢失、和帧类型的有关内容等。

① 通过查看接口的吞吐量可以检测网络的带宽利用状况。如果网络广播信息包的百分比

很高，网络性能开始下降。光纤网转换到以太网段的信息包可能会淹没以太网口。Internet 发生这种情况可以采用优化接口的措施，即在以太网接口使用 `no ip route-cache` 命令，禁用快速转换，并且调整缓冲区和保持队列的设置。

② 两个接口试图同时传输信息包到以太网电缆上时，将发生碰撞。以太网要求冲突次数很少，不同的网络要求是不同的，一般情况下发现冲突每秒有 3~5 次就应该查找冲突的原因了。碰撞冲突产生拥塞，碰撞冲突的原因通常是由于敷设的电缆过长、过分利用、或者“聋”结点。以太网在物理设计和敷设电缆系统管理方面应有所考虑，超规范敷设电缆可能引起更多的冲突发生。

③ 如果接口和线路协议报告运行状态，并且结点的物理连接都完好，可是不能通信。引起问题的原因也可能是两个结点使用了不兼容的帧类型。解决问题的办法是重新配置使用相同帧类型。如果要求使用不同帧类型的同一网络的两个设备互相通信，可以在路由器接口使用子接口，并为每个子接口指定不同的封装类型。

(3) 异步通信口故障排除：互联网络的运行中，异步通信口的任务是为用户提供可靠服务，但又是故障多发部位。异步通信口故障一般的外部因素是：拨号链路性能低劣；电话网交换机的连接质量问题；调制解调器的设置。检查链路两端使用的调制解调器：连接到远程 PC 机端口调制解调器的问题不太多，因为每次生成新的拨号时通常都初始化调制解调器，利用大多数通信程序都能在发出拨号命令之前发送适当的设置字符串；连接路由器端口的问题较多，这个调制解调器通常等待来自远程调制解调器的连接，连接之前，并不接收设置字符串。如果调制解调器丢失了它的设置，应采用一种方法来初始化远程调制解调器。简单的办法是使用可通过前面板配置的调制解调器；另一种方法是将调制解调器接到路由器的异步接口，建立反向 telnet，发送设置命令配置调制解调器。

确定异步通信口故障一般可用下列步骤：检查电缆线路质量；检查调制解调器的参数设置；检查调制解调器的连接速度；检查 `rxspeed` 和 `txspeed` 是否与调制解调器的配置匹配；通过 `show interface async` 命令和 `show line` 命令查看端口的通信状况；从 `show line` 命令的报告检查 EIA 状态显示；检查接口封装；检查信息包丢失及缓冲区丢失情况。

3. 网络故障诊断步骤

(1) 首先确定故障的具体现象，分析造成这种故障现象的原因的类型。例如，主机不响应客户请求服务。可能的故障原因是主机配置问题、接口卡故障或路由器配置命令丢失等。

(2) 收集需要的用于帮助隔离可能故障原因的信息。从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。

(3) 根据收集到的情况考虑可能的故障原因，排除某些故障原因。例如，根据某些资料可以排除硬件故障，把注意力放在软件原因上。

(4) 根据最后的可能故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样可以容易恢复到故障的原始状态。如果一次同时考虑多个故障原因，试图返回故障原始状态就困难多了。

(5) 执行诊断计划，认真做好每一步测试和观察，每改变一个参数都要确认其结果。分析结果确定问题是否解决，如果没有解决，继续下去，直到故障现象消失。

1.4 VPN 实用经验

本节介绍了 VPN 网络的现状与改造措施，并通过具体案例的说明介绍了 VPN 网络在电子政务方面的应用。

1.4.1 VPN 网络解决方案小结

本节将介绍曾经给某市政府（后文中称为“A市”）做的网络改造，使用 VPN 拨号、用智能卡进行身份验证的方式访问上级市委、市政府、省委、省政府、国务院政府网站的完整解决方案，其中涉及到了三层交换机的调试、防火墙的调试、新设备的添加等方面的内容。

A市的网络拓扑如图 1-41 所示，主要分四部分：政府大院、上级政府机关、Internet 网络、乡镇与政府大院外的其他机关（如信访局、检察院、市医院等部门）。

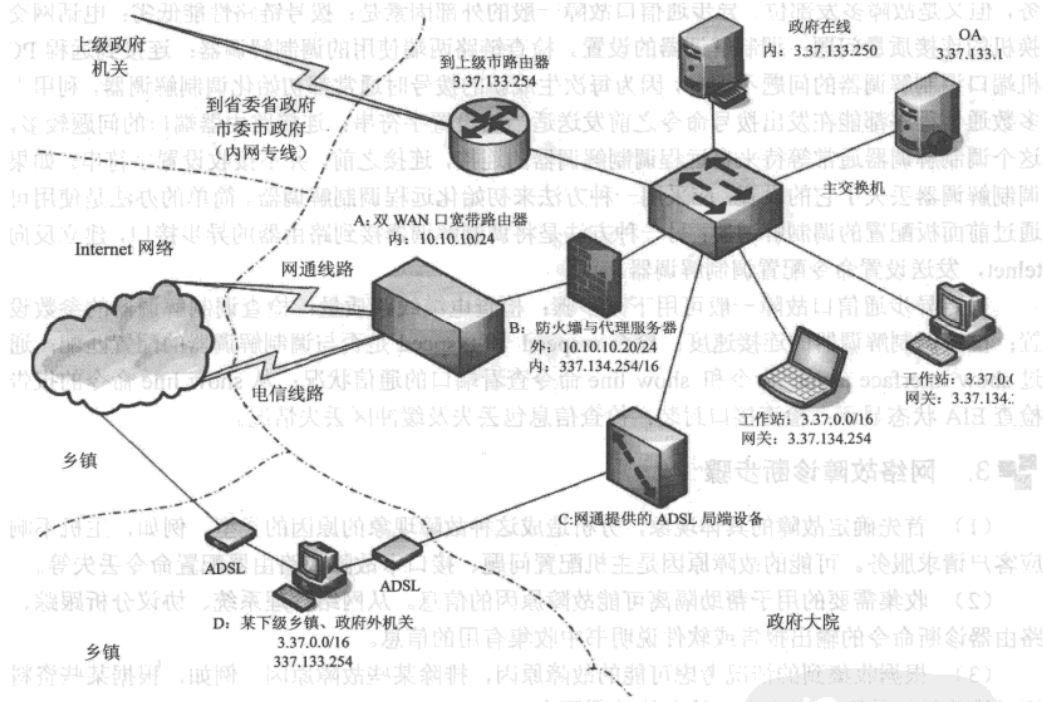


图 1-41 客户网络现状

在“政府大院”区域，在政府信息中心有若干台服务器，其中最主要的有两台服务器，一台为“政府在线”网站，是A市对外的门户网站，是发布到Internet网络的；另一台是“OA”服务器，是A市内部办公自动化网站，是政府内部办公使用，不对外公布（外网不能访问）。政府大院内所有的工作站、服务器没有划分VLAN，所有工作站、服务器都使用3.37.0.0、子网掩码为255.255.0.0的IP地址。

政府中的工作站需要访问Internet与省/市委、省/市政府部门的网站，其中到上级路由器

的内网地址是 3.37.133.254/16，到 Internet 有两个出口，分别为电信与网通的出口，通过一个具有 4 个 LAN 口、两个 WAN 口的路由器连接到 Internet，其中一个 LAN 口接到一台防火墙上，防火墙再接到中心交换机上，该防火墙的内网地址是 3.37.134.254/16，当大院内的计算机需要访问 Internet 时，就将网关地址改为 3.37.134.254，需要访问上级网站时，就将网关地址改为 3.37.133.254。

乡镇的计算机，通过当地网通的 ADSL 接入，其中一个 ADSL 接入到 Internet 网络，另一个 ADSL→通过网通机房→市政府信息中心（由网通提供的）ADSL 局端设备→信息中心交换机→到上级市路由器→上级（省市办公内网）网站。根据图 1-41 所示，该单位“外网（指 Internet 网）”与“政务网（指连接省市网络）”在同一个网络中，没有“分开”。在这种情况下，如果单位中某台计算机在访问 Internet 网络的时候感染了病毒，这台计算机在访问政务网的时候，有可能影响政务网内的其他计算机，对政务网带来安全隐患。

其次，在“政府大院”中所有的计算机、服务器都在同一个网段中，没有划分 VLAN，当某台计算机感染病毒时，尤其是针对操作系统漏洞的病毒，会影响整个网络，现在的网络情况下，每天都有三、四次网络中断，等关掉交换机后再开，网络才会恢复，但过几个小时，整个网络会再次中断。

再次，乡镇与政府大院外的一些部门与机关，都有两条独立的 ADSL（或者其他线路），一条访问 Internet，另一条访问政府内网，许多乡镇为了减少成本，在每个 ADSL 后面接上“宽带共享器”，宽带共享器的“LAN”口再统一接到一个交换机上，乡镇的其他计算机也都接在交换机上，在访问外网与政务网时，通过设置不同的网关地址来访问不同的网络，这也等于将 Internet 与政务网接在一起。另外，采用两条 ADSL 接入，给乡镇带来一定的财务负担。

总之，现在单位的网络问题是：

- （1）外网与政务网在一起，没有“物理”或者“逻辑”分开。
- （2）单位网络经常中断（原因：计算机没有打补丁、没有统一安装杀毒软件）。
- （3）乡镇的财务负担比较重（要承担双倍的上网费用）。

1. 用户需求与网络改造总体方案

如果要对图 1-41 的网络进行改造，让“外网”与“政务网”分开，最好的办法当然是采用双线双机，就是采用两套交换机、两套网线、每个部门或个人两台独立的计算机，一条接政务网交换机，一条接外网交换机上，而乡镇通过光纤的方式直接接入政府信息中心，一条光纤接政务网，一条接外网，乡镇也是配置两套独立的网络、计算机，但这样是不现实的：一是成本太高，二是，即使整个政府大院采用了独立的双线、双机，但到了乡镇一级，或者政府大院外面的单位，他们也会把政务网与外网接在一起，即使外面把网络接在一起，以目前的技术水平也是检查不出来的。

为了解决前面提出的三个问题，决定采用如下的方案：

（1）在政府大院主交换机与上级路由器之间增加一台 VPN 服务器，默认情况下，允许所有的计算机访问 Internet 网络，当需要访问政府网时，通过 VPN 拨号的方式拨到 VPN 服务器，通过 VPN 服务器访问政务网。在拨号后，将自动断开与 Internet 网络的连接。

（2）对于乡镇用户来说，撤销到政府信息中心的 ADSL 线路，而是通过网通提供的 Internet 网络接入，采用 VPN 拨号的方式，通过“政府信息中心”的电信或者网通的出口，拨号政府信息中心提供的 VPN 服务器，通过 VPN 服务器访问政务网，当乡镇的计算机拨叫到 VPN 服

网管天下 网管经验谈

务器后，因为路由信息的改变，也不能访问 Internet；当断开 VPN 连接后，即恢复到 Internet 的访问。

(3) 增加的 VPN 服务器，具有 3 个接口：一个接政务内网路由器，一个接政府大院主交换机（为政府大院内部用户提供 VPN 接口），一个接政府信息中心双 WAN 口路由器（为乡镇用户提供接口）。

为了解决操作系统打补丁问题，同时为了统一解决杀毒软件问题，再增加一台服务器，在这台服务器上安装 WSUS 与网络版杀毒软件（或者经过改造的单机版杀毒软件，例如金山毒霸、卡巴斯基、NOD32 等），为单位的所有操作系统提供补丁与杀毒软件的升级服务。

(4) 因为整个政府大院在同一个局域网中，当网络中的一台计算机出现问题时，可能会感染整个网络，为了解决这个问题，将主交换机用一台三层交换机代替，对政府大院内的所有计算机，根据楼层与单位划分 VLAN，基本上每个楼层、每个部门在同一个 VLAN 中，服务器在一个单独的 VLAN 中。

改造后的网络拓扑如图 1-42 所示。

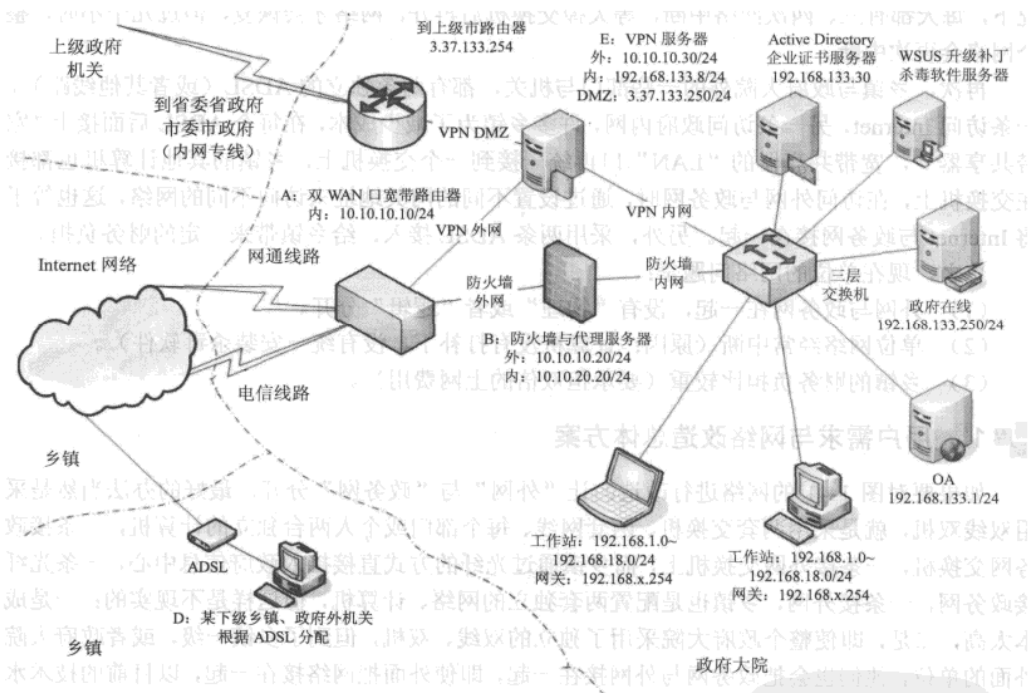


图 1-42 改造后网络拓扑

在图 1-42 中，总体来说，没有对网络进行大的硬性改造，只是将政府大院的主交换机更换为“三层交换机”，增加三台服务器（一台 VPN 服务器——3 块网卡，一台 WSUS 与杀毒软件服务器——单块网卡，一台 Active Directory 与企业证书服务器——单块网卡），其中 WSUS 与 Active Directory 服务器接在核心交换机上，与原来的 OA、政府在线网站在同一个 VLAN 中。

除了要调试新增加的三层交换机外，还需要调整图 1-42 中双 WAN 口的路由器，将 VPN

所需要的端口 TCP 的 1723 与 UDP 的 4500 映射到 VPN 服务器所使用的 IP 地址上，在本节中，VPN 服务器“外网”网卡使用了 10.10.10.30/24 的 IP 地址。

2. 网络改造具体方案

在具体的改造中，涉及到 Internet 出口（双 WAN 口路由器）的调试、新购买的三层交换机的调试和 VPN 服务器的调试，因为重新调整了单位内网的地址，所以单位原来的防火墙与代理服务器的地址也要做改动。之所以修改原来单位使用的内网地址 3.37.0.0/16，原因有二：第一个原因是 3.37.0.0 并不是私有的内网地址，这个地址在 Internet 上是存在的，在内网中推荐使用 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 的地址段；第二个原因是划分 VLAN 后，为了与省、市政务网通，使用私有的地址，可以方便新购买的三层交换机、上级路由器的调试。

（1）交换机的设置。

下面是华为 3600 系列三层交换机的配置，根据楼层、单位的数量，将政府大院划分为 18 个 VLAN，其中 192.168.1.0~192.168.18.0/24 为工作站使用，192.168.133.0/24 为服务器使用，10.10.20.20/24 为 VLAN1001，划分在一个千兆位端口上，专门接防火墙用，防火墙的内网地址改为 10.10.20.20/24，另一个千兆位端口接 VPN 服务器内网。

说
明

在下面的配置中，凡是以//开头的都为注释部分，用来说明上一行配置的意思。

```
sysname HW3600
#
vlan 1
#
vlan 1001
//创建 VLAN1001
description "FangHuoQiang"
//设置描述信息，“防火墙”的拼音，表示到防火墙的 VLAN
#
vlan 1005
description "Server-8Lou"
//表示 8 楼，服务器区 VLAN
#
vlan 2811
description "JiJianWei-Yilou"
//纪检委-1 楼
#
vlan 2812
description "XinFangJu-Yilou"
//信仿局-1 楼
#
vlan 2813
description "Qita-Yilou"
//1 楼其他，表示在 1 楼的其他部门
#
vlan 2821
```



```
description "NongGongWei-2Lou"
//农工委-2楼
#
vlan 2822
description "ZhengXie-2Lou"
//政协-2楼
#
vlan 2823
description "Qita-2Lou"
//2楼其他
#
vlan 2831
description "RenDa-3Lou"
//人大-3楼
#
vlan 2832
description "Qita-3Lou"
#
vlan 2841
description "Qita-4Lou"
#
vlan 2851
description "ShiZhengFu-5Lou"
//市政府-5楼
#
vlan 2861
description "ShiWei-6Lou"
//市委-6楼
#
vlan 2871
description "ZuZhiBu-7Lou"
//组织部-7楼
#
vlan 2881
description "KeJiJu-8Lou"
//科技局-8楼
#
vlan 2882
description "ZhengFaWei-8Lou"
//政法委-8楼
#
vlan 2883
description "Qita-8Lou"
//其他部门-8楼
#
vlan 2884
description "XinXiZhongXin-8Lou"
//信息中心-8楼
#
interface Vlan-interface1001
ip address 10.10.20.10 255.255.255.0
设置与防火墙相连的交换机的端口地址是 10.10.20.10
```



```
#
interface Vlan-interface1005
ip address 192.168.133.254 255.255.255.0
//设置服务器所属 VLAN 的端口地址 192.168.133.254
#
interface Vlan-interface2811
ip address 192.168.1.254 255.255.255.0
#
interface Vlan-interface2812
ip address 192.168.2.254 255.255.255.0
#
interface Vlan-interface2813
ip address 192.168.3.254 255.255.255.0
#
interface Vlan-interface2821
ip address 192.168.4.254 255.255.255.0
#
interface Vlan-interface2822
ip address 192.168.5.254 255.255.255.0
#
interface Vlan-interface2823
ip address 192.168.6.254 255.255.255.0
#
interface Vlan-interface2831
ip address 192.168.7.254 255.255.255.0
#
interface Vlan-interface2832
ip address 192.168.8.254 255.255.255.0
#
interface Vlan-interface2841
ip address 192.168.9.254 255.255.255.0
#
interface Vlan-interface2851
ip address 192.168.10.254 255.255.255.0
#
interface Vlan-interface2861
ip address 192.168.11.254 255.255.255.0
#
interface Vlan-interface2871
ip address 192.168.12.254 255.255.255.0
#
interface Vlan-interface2881
ip address 192.168.13.254 255.255.255.0
#
interface Vlan-interface2882
ip address 192.168.14.254 255.255.255.0
#
interface Vlan-interface2883
ip address 192.168.15.254 255.255.255.0
#
interface Vlan-interface2884
```

网管天下 网管经验谈

```
ip address 192.168.18.254 255.255.255.0
#
interface Aux1/0/0
#
interface Ethernet1/0/1
port access vlan 2811
//第1个端口属于VLAN2811
#
interface Ethernet1/0/2
port access vlan 2812
#
interface Ethernet1/0/3
port access vlan 2813
#
interface Ethernet1/0/4
port access vlan 2821
#
interface Ethernet1/0/5
port access vlan 2822
#
interface Ethernet1/0/6
port access vlan 2823
#
interface Ethernet1/0/7
port access vlan 2831
#
interface Ethernet1/0/8
port access vlan 2832
#
interface Ethernet1/0/9
port access vlan 2841
#
interface Ethernet1/0/10
port access vlan 2851
#
interface Ethernet1/0/11
port access vlan 2861
#
interface Ethernet1/0/12
port access vlan 2871
#
interface Ethernet1/0/13
port access vlan 2881
#
interface Ethernet1/0/14
port access vlan 2882
#
interface Ethernet1/0/15
port access vlan 2883
#
interface Ethernet1/0/16
port access vlan 2884
```

```
#
interface Ethernet1/0/17
port access vlan 1005
#
interface Ethernet1/0/18
port access vlan 1005
#
interface Ethernet1/0/19
port access vlan 1005
#
interface Ethernet1/0/20
port access vlan 1005
#
interface Ethernet1/0/21
port access vlan 1005
#
interface Ethernet1/0/22
port access vlan 1005
#
interface Ethernet1/0/23
port access vlan 1003
#
interface Ethernet1/0/24
port access vlan 1005
#
interface GigabitEthernet1/1/1
#
interface GigabitEthernet1/1/2
#
interface GigabitEthernet1/1/3
port access vlan 1001
#
interface GigabitEthernet1/1/4
port access vlan 1005
#
undo irf-fabric authentication-mode
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.10.20.20
//添加静态路由，这是访问 Internet 网络的接口设置
//下面这几条设置的静态路由，是到政务网的路由
ip route-static 3.0.0.0 255.0.0.0 192.168.133.8
ip route-static 66.0.0.0 255.0.0.0 192.168.133.8
ip route-static 68.0.0.0 255.0.0.0 192.168.133.8
ip route-static 172.18.0.0 255.255.0.0 192.168.133.8
ip route-static 200.0.0.0 255.0.0.0 192.168.133.8
#
```

(2) 到上级路由器与防火墙代理服务器的调试。

由于在 VPN 服务器中，新增加了一个 DMZ 的接口，该接口继续使用原来的 IP 地址，所

网管天下 网管经验谈

以，“到上级市路由器”不需要设置。需要设置的是图 1-43 中“A：双 WAN 口宽带路由器”，因为 VPN 服务器要对 Internet 网上的用户提供服务（主要是乡镇、政府大院以外的其他机关），所以，需要在双 WAN 口的宽带路由器上，映射 VPN 服务所需要的端口到 VPN 服务器的“外网”地址，即 10.10.10.30。VPN 服务器所需要的端口，如表 1-1 所示。

表 1-1 VPN 服务器所需端口一览表

服务描述	协议	端口	方向
PPTP 服务器	TCP	1723	入站
IPSec NAT-T 服务器	UDP	4500	接收发送
IKE 服务器	UDP	500	接收发送
L2TP 服务器	UDP	1701	接收发送

表 1-1 中的这几项协议并不是必须的，例如，如果客户端使用 PPTP 方式拨入，只需要映射“PPTP 服务器”与“IPSec NAT-T 服务器”即可，如果客户端使用 L2TP 方式拨入，需要映射“L2TP 服务器”、“IKE 服务器”与“IPSec NAT-T 服务器”。如果你不清楚 VPN 服务器的类型，发布上面的这 4 个端口即可，在一些防火墙与路由器中，端口的“方向”可能不容易掌握，那就做端口的完全映射即可。

3. VPN 服务器组建

VPN 服务器的组建包括 Active Directory 服务器、企业证书服务器、VPN 服务器的安装，主要包括 VPN 服务器的安装配置，下面将详细介绍。

(1) 服务器的总体设置。

在做好三层交换机与双 WAN 口宽带路由器的设置后，接下来就是 Active Directory 服务器、企业证书服务器与 VPN 服务器的安装配置了，为了更容易说明问题，将图 1-42 简化为图 1-43，这是需要设置的两台服务器。

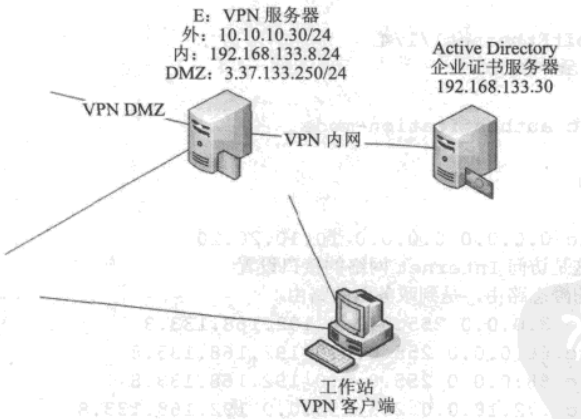


图 1-43 简化设置

在图 1-43 中，需要两台服务器，一台服务器做 Active Directory 与证书服务器，另一台做 VPN 服务器，还需要一台工作站进行测试，当这台工作站需要模拟内网环境时，设置为内网

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

地址拨叫 VPN 服务器的“内网”地址，当需要模拟 Internet 网络环境时，设置成外网地址拨叫 VPN 服务器的“外网”地址。各服务器的具体参数，如表 1-2 所示。

表 1-2 各服务器的具体参数

顺 序	计 算 机 名	IP 地址/24	DNS 地址	DNS 域名	描 述
1	AD-SERVER	192.168.133.30	192.168.133.30	aa.gov.cn	域控制器、证书服务器
2	VPN-Server	192.168.133.8	192.168.133.30	aa.gov.cn	内网网卡
		10.10.10.30			外网网卡
		3.37.133.250			DMZ 区网卡
3	XP	10.10.10.50			VPN 客户端
		192.168.133.50			

(2) Active Directory 服务器与证书服务器的安装与配置。

在将要做 Active Directory 服务器与证书服务器的计算机上，进行下面的主要操作：

- 安装 Windows Server 2003 的标准版或者企业版。
- 修改计算机名称。
- 设置 IP 地址。
- 升级到 Active Directory。
- 安装企业证书服务器

主要步骤如下。

第 1 步，修改计算机名称为 ad-server，并重新启动计算机。

第 2 步，设置 IP 地址为 192.168.133.30，子网掩码为 255.255.255.0，设置 DNS 为 127.0.0.1（代表本机地址，也可以设置为 192.168.133.30）。

说
·
明

在实际使用中，必须要根据实际情况设置网关地址。

第 3 步，接下来要将计算机升级到“Active Directory（活动目录）”，并设置域名为 aa.gov.cn。

升级到 Active Directory 后，单击“立即重新启动”按钮，重新启动 Windows Server 2003 的计算机，完成 Active Directory 的安装。

第 4 步，重新启动计算机并再次进入系统后，在“控制面板→添加/删除程序→添加/删除 Windows 组件”中，先安装（选中）“应用程序服务器→ASP.NET 和 Internet 信息服务”。然后再安装企业根证书服务，单击“下一步”按钮，在“CA 类型”页中，选择“企业根 CA”。

在“CA 识别信息”页中，在“此 CA 的公用名称”文本框中，输入该企业根 CA 的信息，例如 ent-ca.aa.gov.cn，这个信息将在用 IE 申请证书时出现在证书申请首页中，并且最好将这个名称注册为 DNS 域名对外提供服务，在“有效期限”页中，选择该证书服务器的有限期限，默认为 5 年，可以根据需要修改，如图 1-44 所示。

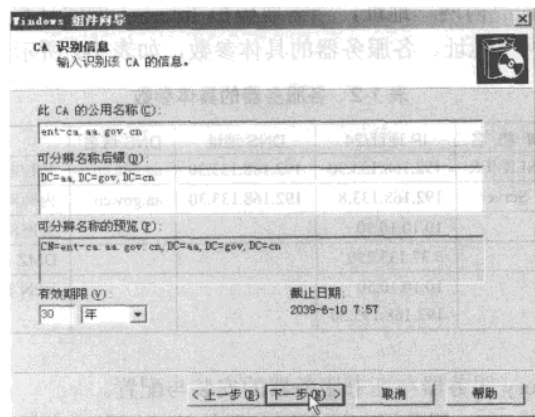


图 1-44 CA 识别信息

第 5 步，在安装完成后，在 IE 浏览器中，输入 <http://192.168.133.30/certsrv>（其中 192.168.133.30 是证书服务器的 IP 地址），按 Enter 键，首先会弹出身份验证对话框，输入管理员账户和密码，如图 1-45 所示。然后按 Enter 键，进入企业证书申请页，首先在“Microsoft 证书服务器”后面显示的名称就是图 1-44 中输入的信息，如图 1-46 所示。

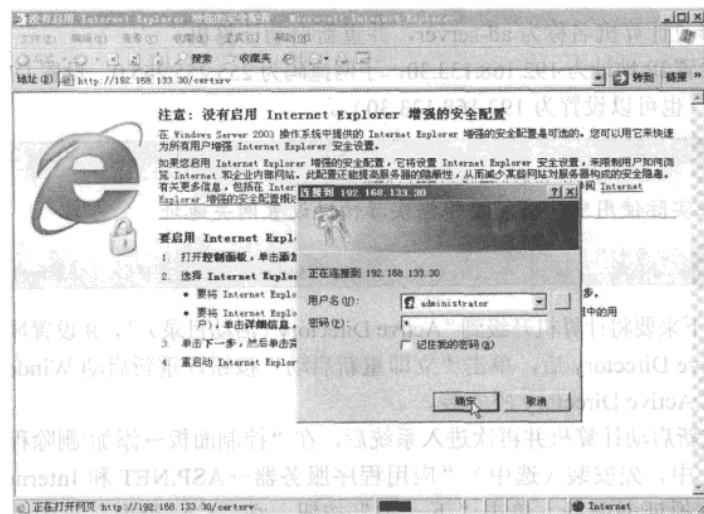


图 1-45 输入账户和密码

至此，Active Directory 服务器与企业证书服务器的配置基本完成，接下来将讲述 VPN 服务器的配置过程。

4. 准备 VPN 服务器

在准备做 VPN 服务器的计算机上，需要经过一系列步骤的配置，才可以让 VPN 服务器使用智能卡进行身份验证，这些步骤主要有：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 修改计算机名称并重启。
- 设置 IP 地址与 DNS 地址。
- 将计算机加入到 Active Directory 服务器。
- 安装 ISA Server。
- 申请证书。
- 启用 VPN 服务。

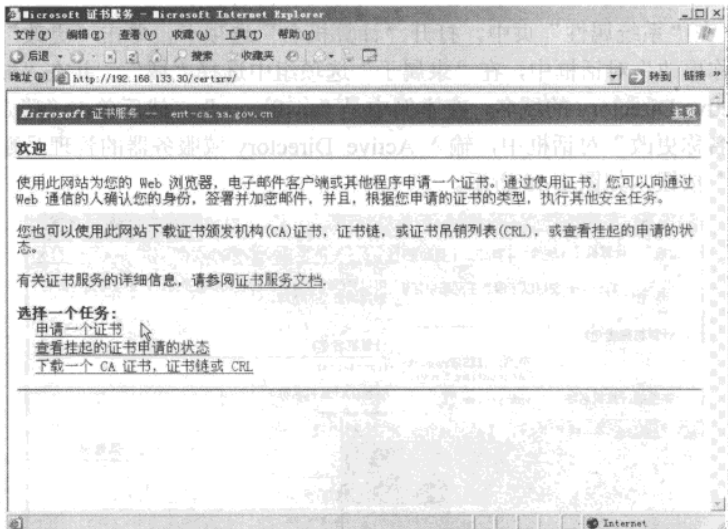


图 1-46 企业证书申请页

(1) VPN 服务器基本准备。

在准备做 VPN 服务器的计算机上，首先设置内网网卡的 IP 地址为 192.168.133.8，设置 DNS 地址为 192.168.133.30，设置该网卡名称为“LAN”；设置外网网卡的 IP 地址为 10.10.10.30，设置网关地址为 10.10.10.10，将外网网卡重命名为“Internet”；设置第三块网卡 IP 地址为 3.37.133.250，设置该网卡名称为“DMZ”。

然后重命名计算机为 VPN-Server，之后重新启动计算机，如图 1-47 所示。

最后，确认该计算机没有安装 IIS、没有启用 Windows 内置的防火墙与没有启用“路由和远程访问”服务。

(2) 将计算机加入到 Active Directory。

将计算机加入到 Active Directory，作为域 aa.gov.cn 的成员服务器，其主要步骤如下。

第 1 步，进入命令提示符，使用 ping 命令，测试到 Active Directory 服务器(192.168.133.30)

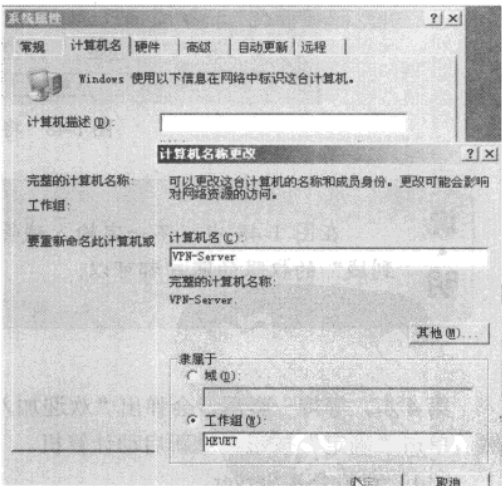


图 1-47 修改计算机名称并重启计算机

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

连接正常。当连接正常时，继续后面的操作。

说明

在使用 ping 命令时，最好是 ping ad-server.aa.gov.cn，看 DNS 的解析是否正常，ad-server.aa.gov.cn 是 Active Directory 的域服务器的名称。

第 2 步，用鼠标右键单击“我的电脑”，从弹出的快捷菜单中选择“属性”命令。

第 3 步，在“系统属性”页中，打开“计算机名”选项卡，单击“更改”按钮，在弹出的“计算机名称更改”对话框中，在“隶属于”选项组中选择“域”，并在“域”文本框中输入要加入的 Active Directory 的域名，在本例中是“msft.com”，然后单击“确定”按钮，在弹出的“计算机名称更改”对话框中，输入 Active Directory 域服务器的管理员账户的名称，然后单击“确定”按钮，如图 1-48 所示。

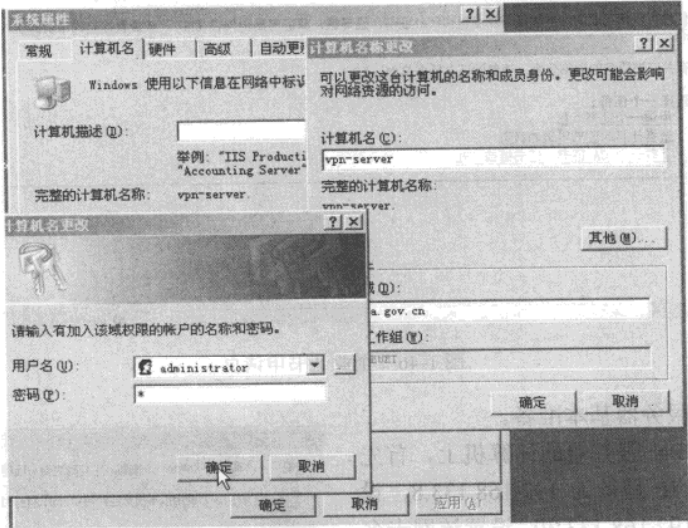


图 1-48 将计算机加入到域

说明

在图 1-48 中，不一定输入域管理员账户的名称，只要具有“将计算机加入到域”的权限的账户都可以。

第 4 步，等待一会后，会弹出“欢迎加入 aa.gov.cn 域”对话框，单击“确定”按钮返回，然后单击“确定”按钮，重新启动计算机。

(3) 安装 ISA Server。

当计算机再次登录时，请以域管理员的身份登录到域，如图 1-49 所示。

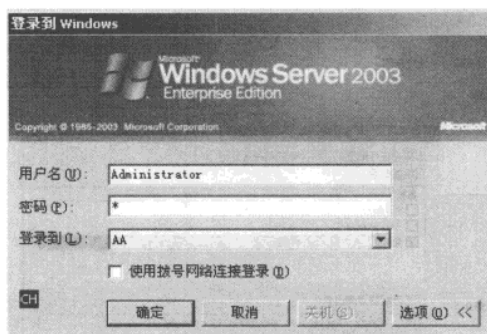


图 1-49 登录到域

在安装 ISA Server 之前，添加到内网、DMZ 区的静态路由。因为在局域网中包括的网段是 192.168.1.0~192.168.18.0/24，到 DMZ 区（上级政府网）包括 3.0.0.0/8、60.0.0.0/8、66.0.0.0/8、68.0.0.0/8、200.0.0.0/8，进入命令提示符，使用 route 命令——添加到这些网段的静态路由，其命令如下：

```
route add -p 192.168.0.0 mask 255.255.224.0 192.168.133.254
route add -p 3.0.0.0 mask 255.0.0.0 3.37.133.254
route add -p 60.0.0.0 mask 255.0.0.0 3.37.133.254
route add -p 66.0.0.0 mask 255.0.0.0 3.37.133.254
route add -p 68.0.0.0 mask 255.0.0.0 3.37.133.254
route add -p 200.0.0.0 mask 255.0.0.0 3.37.133.254
```

说
明

① 添加的第一条静态路由 192.168.0.0 mask 255.255.224.0 包括了从 192.168.0.0 ~ 192.168.31.0/24 的地址段，这样已经包括了 192.168.1.0 ~ 192.168.18.0/24，并且 192.168.19.0 ~ 192.168.31.0/24 在实际中也没有使用，这样是不影响正常使用的，所以可以这样配置。

② 最好在安装 ISA Server 2006 之前添加静态路由，如果在安装 ISA Server 之前忘记添加静态路由，也可以在安装 ISA Server 之后配置。但在安装 ISA Server 2006 更改 IP 地址、路由信息时，需要重新配置 ISA Server 的“网络”，有关这些内容，本节不做过多介绍。

然后开始安装 ISA Server 2006，在安装的过程中需要注意以下几点：

第 1 步，选择“lan”网卡为内部网络，如图 1-50 所示。

在选择“lan”时，在“网络适配器详细信息”中会显示路由信息。

第 2 步，其他采用默认安装，将不再介绍。

(4) 申请证书。

在配置 VPN 服务器之前，需要为该服务器申请一个“计算机证书”，但因为这台计算机安装了 ISA Server，默认是阻止这台计算机访问其他服务器的，所以需要创建访问策略。

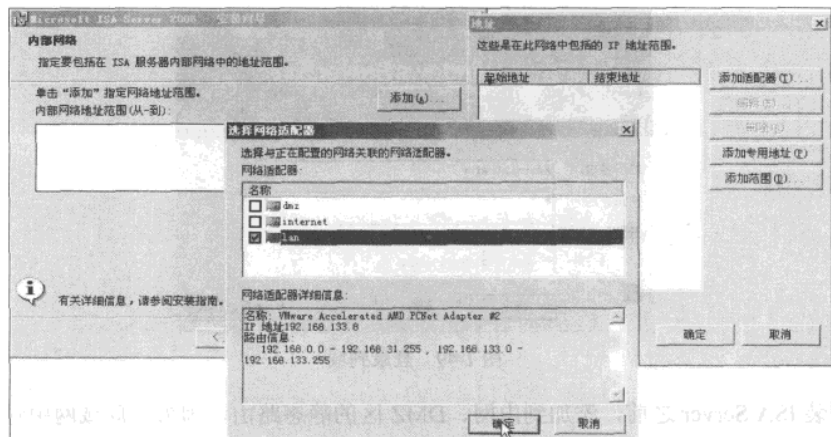


图 1-50 选择内部网络

打开 ISA Server 服务器，创建一条策略，该策略允许 Active Directory 服务器（IP 地址为 192.168.133.30）的计算机与 ISA Server 服务器（即 VPN 服务器）可以以任意协议“互相”通信，如图 1-51 所示。

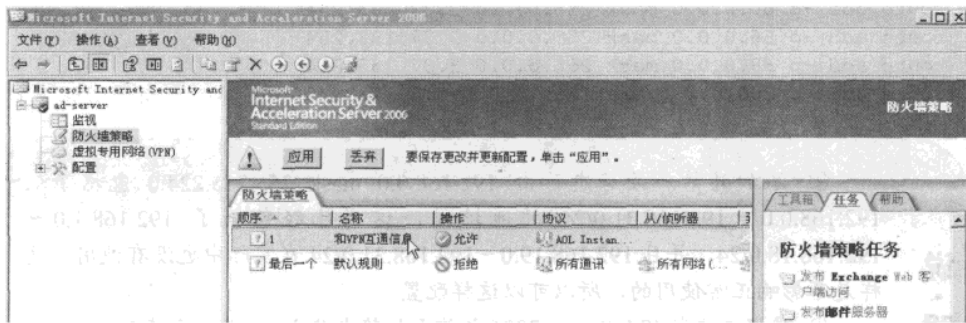


图 1-51 创建策略：允许与 AD 以任意协议互相通信

在创建访问规则之后，就可以为 VPN 服务器从“企业证书服务器”申请“计算机证书”，主要步骤如下：

第 1 步，在 VPN 服务器计算机上，打开 IE 浏览器，输入 <http://192.168.133.30/certsrv>，在弹出的对话框中输入域管理员账户和密码。

第 2 步，在“欢迎”页中单击“申请一个证书”链接；在“申请一个证书”页中单击“高级证书申请”链接；在“高级证书申请”页中单击“创建并向此 CA 提交一个申请”链接。

第 3 步，然后打开“系统属性”对话框，查看并复制计算机名称，如图 1-52 所示。

第 4 步，切换到高级证书申请页，在“高级证书申请”页中，在“证书模板”下拉列表框中选择“Web 服务器”，在“姓名”文本框中“粘贴”图 1-47 中复制的计算机名称（如图 1-53 所示），选中“将证书保存在本地计算机存储中”复选框，然后单击“提交”按钮，如图 1-54 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

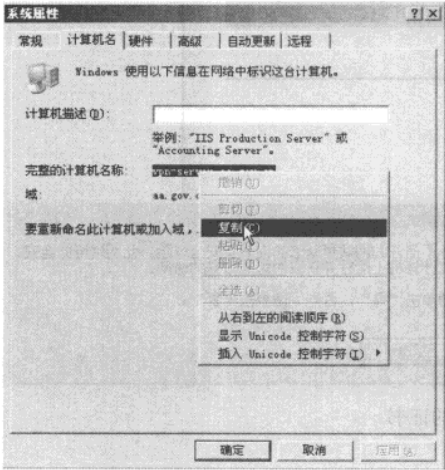


图 1-52 复制计算机名称

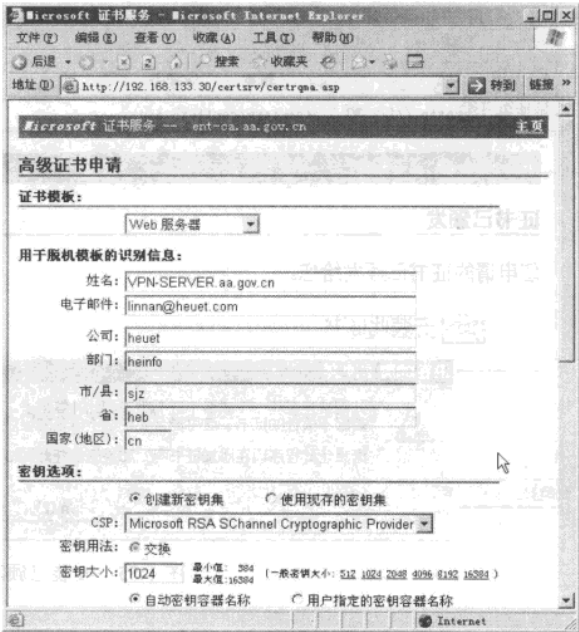


图 1-53 输入正确的计算机名称

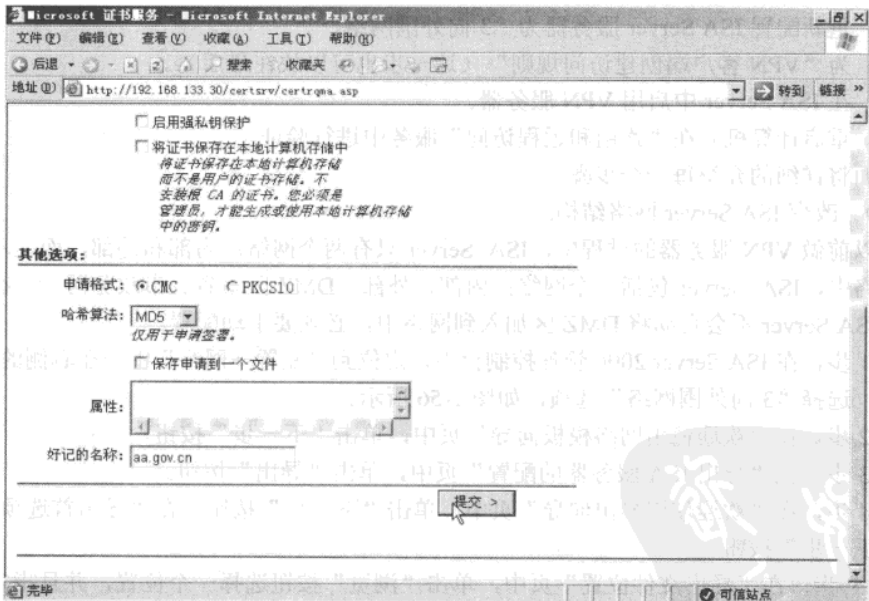


图 1-54 将证书保存在本地计算机存储中

第 5 步，从企业证书服务器申请证书时，证书会立刻颁发。在“证书已颁发”页中单击“安装此证书”链接，在弹出的“潜在脚本冲突”中单击“是”按钮，如图 1-55 所示。

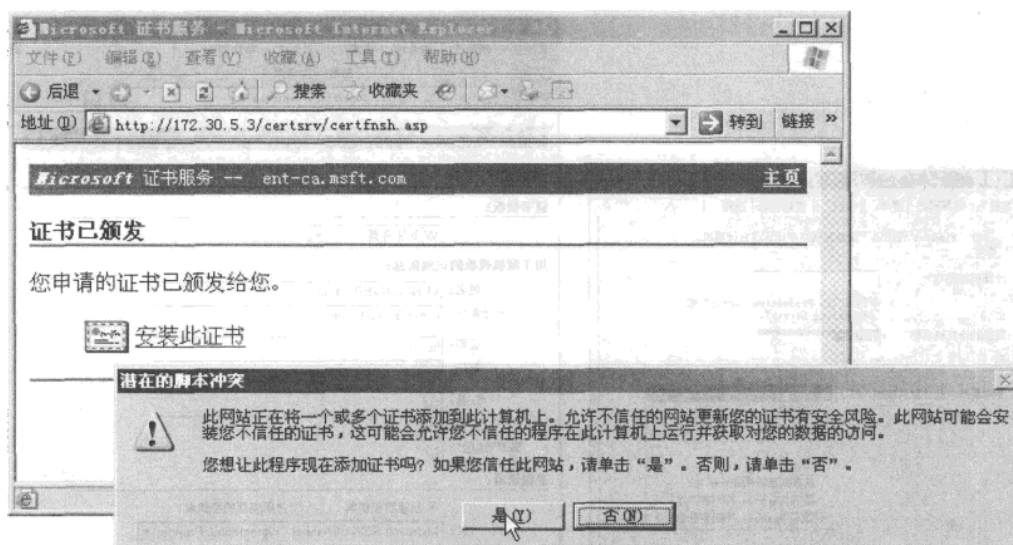


图 1-55 安装已颁发的证书

5. 启用 VPN 服务

在申请并安装证书之后，就可以在 ISA Server 中启用 VPN 服务器了，主要步骤包括：

- 重新配置 ISA Server 服务器为“3 向外围网络”。
- 为“VPN 客户端创建访问规则”（这一步也可以放在最后）。
- 在 ISA Server 中启用 VPN 服务器。
- 重启计算机并在“路由和远程访问”服务中进行验证。

下面将详细的介绍每一个步骤。

（1）改变 ISA Server 网络结构。

在以前做 VPN 服务器的过程中，ISA Server 只有两个网络：内部和外部，而在本章所描述的网络中，ISA Server 包括 3 个网络：内部、外部、DMZ 区（省、市政政务网）。在默认情况下，ISA Server 不会自动将 DMZ 区加入到网络中，必须要手动配置。

第 1 步，在 ISA Server 2006 管理控制台中，定位到“配置→网络”中，在右侧的“模板”窗格中，选择“3 向外围网络”选项，如图 1-56 所示。

第 2 步，在“欢迎使用网络模板向导”页中，单击“下一步”按钮。

第 3 步，在“导出 ISA 服务器的配置”页中，单击“导出”按钮。

第 4 步，在“欢迎使用导出向导”页中，单击“下一步”按钮；在“导出首选项”页中，单击“下一步”按钮。

第 5 步，在“导出文件位置”页中，单击“浏览”按钮选择一个位置，并且指定一个导出的文件名，然后单击“下一步”按钮。在“正在完成导出向导”页中，单击“完成”按钮。

第 6 步，在“内部 网络 IP 地址”页中，选择“内网”地址网卡，如图 1-57 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

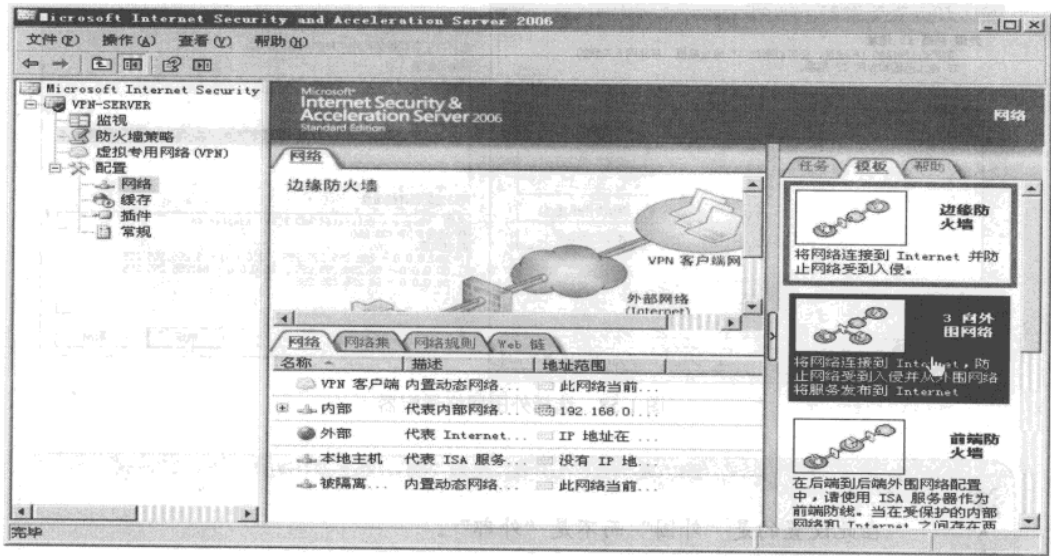


图 1-56 3 向外围网络

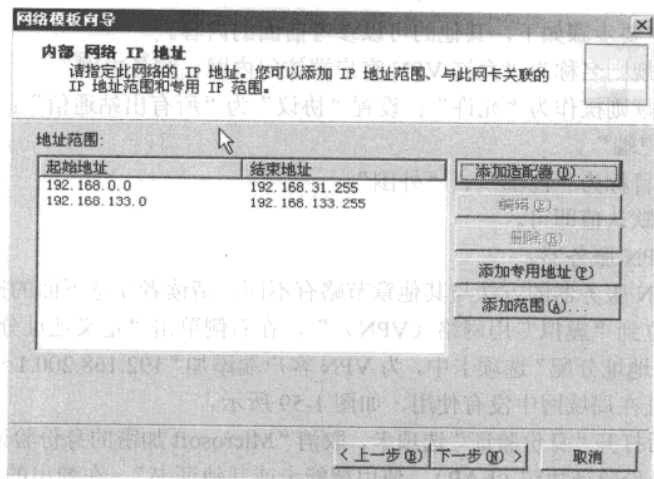


图 1-57 选择内网网络地址

- 第 7 步，在“外围 网络 IP 地址”页中，添加外围网卡适配器，如图 1-58 所示。
 - 第 8 步，在“选择一个防火墙策略”页中，选择“阻止所有访问”，然后单击“下一步”按钮。
 - 第 9 步，在“正在完成网络模板向导”页中，单击“完成”按钮。
 - 第 10 步，单击“应用”按钮，让设置生效。
- 在完成 3 向网络配置后，导入第 3~5 步中导出的 ISA Server 设置。
- (2) 为 VPN 客户端创建访问规则。
- 在本节示例中，将允许 VPN 客户端访问“内部”与“外围”。

网管天下 网管经验谈

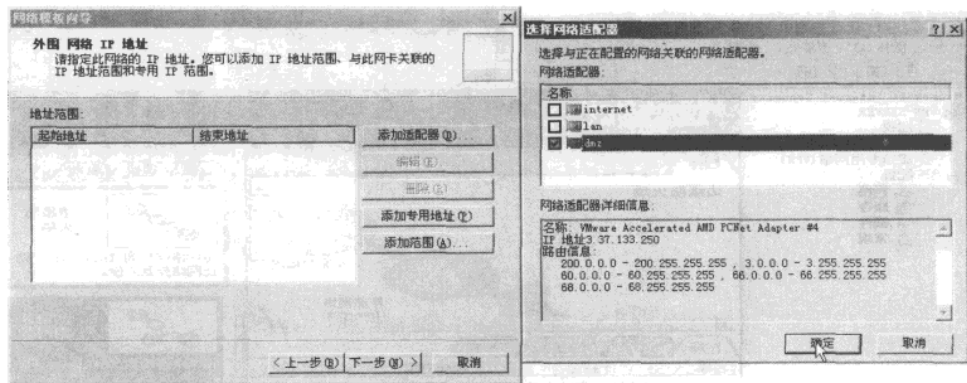


图 1-58 选择外围网络适配器

注
·
意

在此设置的是“外围”而不是“外部”。

创建规则的主要步骤如下，其他的可以参考前面的内容。

- ① 设置访问规则名称为“允许 VPN 客户端访问内网、政务内网”。
 - ② 设置访问规则操作为“允许”；设置“协议”为“所有出站通信”；在“访问规则源”中选择“VPN 客户端”。
 - ③ 访问规则目标为“内部”、“外围”。
 - ④ 其他选择默认值即可。
- (3) 启用 VPN 服务器。

本节配置 VPN 服务器的方法与其他章节略有不同，请读者注意下面的操作。

第 1 步，定位到“虚拟专用网络 (VPN)”，在右侧单击“定义地址分配”链接。

第 2 步，在“地址分配”选项卡中，为 VPN 客户端添加“192.168.200.1~192.168.250.255”的地址，这个地址在局域网中没有使用，如图 1-59 所示。

第 3 步，然后打开“身份验证”选项卡，取消“Microsoft 加密的身份验证版本 2”的选择，选中“可扩展的身份验证协议 (EAP)，使用智能卡或其他证书”，在弹出的对话框中单击“确定”按钮，然后再次单击“确定”按钮。

第 4 步，在“访问网络”选项卡中，选中“内部”与“外部”，因为该 VPN 服务器，也要为“内部”用户提供 VPN 服务，如图 1-60 所示。然后单击“确定”按钮，返回 ISA Server 管理控制台。

第 5 步，在 ISA Server 管理控制台中，在右侧的任务窗格中单击“配置 VPN 客户端访问”链接，在弹出的“VPN 客户端 属性”页中，选中“启用 VPN 客户端访问”单选按钮，在“允许的最大 VPN 客户端数量”文本框中输入该 VPN 服务器最大的并发连接数，例如 2000，然后单击“确定”按钮，在弹出的对话框中单击“确定”按钮。

第 6 步，单击“应用”按钮，让设置生效。

第 7 步，重新启动计算机。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

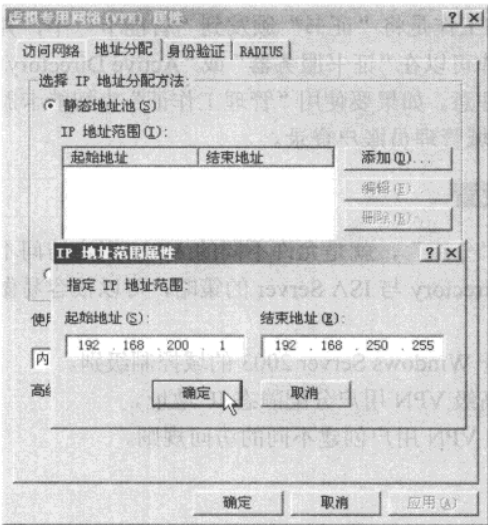
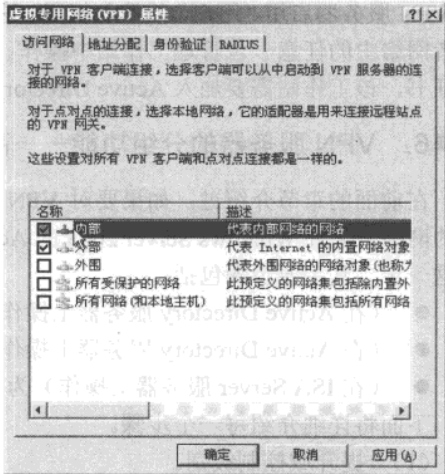


图 1-59 创建静态地址



网管天下 网管经验谈

至此，VPN 服务器端的配置完成，接下来的工作是将“证书”颁发到“智能卡”中，并为 VPN 服务器启用“用户”的拨入权限，这些操作可以在“证书服务器”或“Active Directory”或者网络中的任意一台管理工作站中操作。需要注意，如果要使用“管理工作证”为智能卡颁发证书，该工作站需要加入 Active Directory 并以域管理员账户登录。

6. VPN 服务器的分组功能——高级设置

在前面的章节介绍过，如果要对 VPN 用户“分组”，就是允许不同的 VPN 用户访问不同的网络，配置 Windows Server 2003 的 Active Directory 与 ISA Server 的策略，可以很容易做到这一步，其主要步骤包括：

- （在 Active Directory 服务器上操作）提升 Windows Server 2003 的域控制级别。
- （在 Active Directory 服务器上操作）为高级 VPN 用户分配静态 IP 地址。
- （在 ISA Server 服务器上操作）为不同的 VPN 用户创建不同的访问规则。

下面将详细介绍每一个步骤。

(1) 提升域控制级别。

第 1 步，切换到 Active Directory 服务器上，在“Active Directory 用户和计算机”上，用鼠标右键单击域名，从弹出的快捷菜单中选择“提升域功能级别”，如图 1-62 所示。

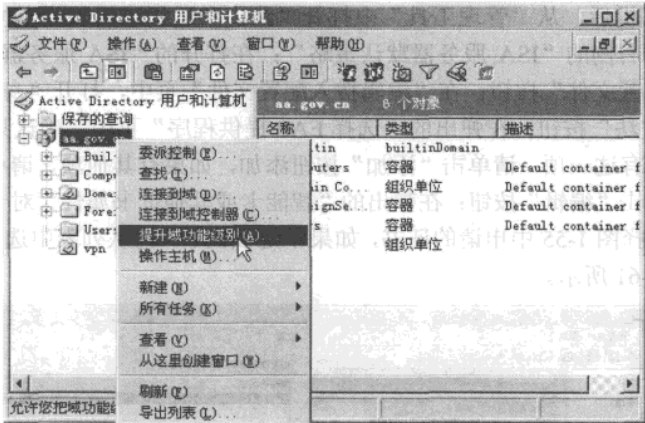


图 1-62 提升域功能级别

第 2 步，在弹出的“提升域功能级别”对话框中，在“选择一个可用的域功能级别”下拉列表框中选择“Windows Server 2003”选项，然后单击“提升”按钮，如图 1-63 所示。

第 3 步，在弹出的“提升域功能级别”警告框中单击“确定”按钮，如图 1-64 所示。

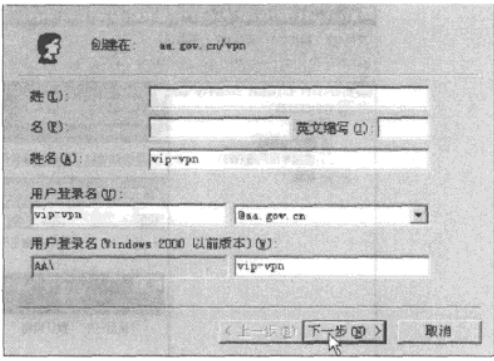
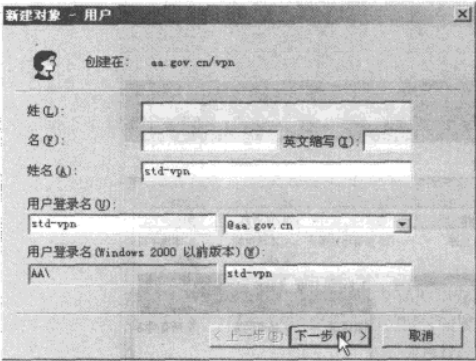
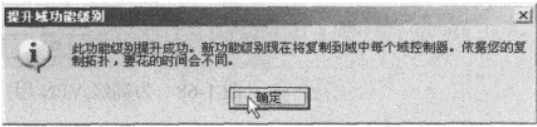
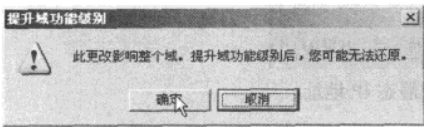
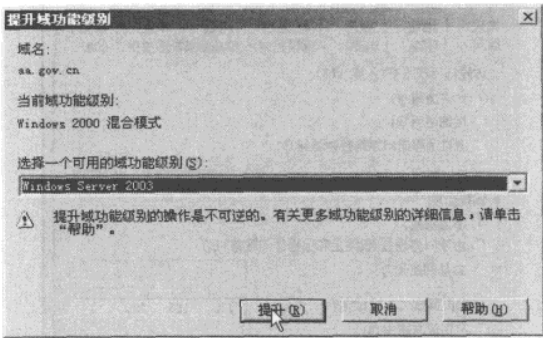
第 4 步，在提升成功后，弹出如图 1-65 所示对话框，单击“确定”按钮。

为了让设置立刻生效，重新启动计算机。

(2) 为 VPN 用户分配静态 IP 地址。

第 1 步，当再次进入后，打开“Active Directory 用户和计算机”，创建两个 VPN 用户，一个名为 std-vpn，另一个为 vip-vpn，这两个用户，前面 std-vpn 对应“标准 VPN 用户”，后一个用户“vip-vpn”对应“高级 VPN 用户”，如图 1-66 和图 1-67 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第 2 步，对于“普通 VPN”用户，只允许其有“拨入”权限即可，而对于“高级 VPN”用户，在设置其属性是，除了设置“允许访问”权限外，还要选中“分配静态 IP 地址”，并且为“高级 VPN 用户”使用在图 1-59 中“比较靠后”的地址，例如，使用 192.168.220.1~192.168.220.255 的地址，从此地址段中为“高级 VPN 用户”设置一个静态地址，如图 1-68 所示。

对于网络中的每一个“高级 VPN 用户”，都要为其分配一个静态地址，并且静态地址不能与其他用户的重复，最好这些地址在一个范围内。

(3) 在 ISA Server 上创建不同的访问策略。

返回到 ISA Server 服务器上，禁用原来的 VPN 访问策略，并创建两个新的策略。

- 允许“标准 VPN 用户”地址范围的用户访问指定的地址范围的计算机。
- 允许“高级 VPN 用户”地址范围的用户访问所有的计算机。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

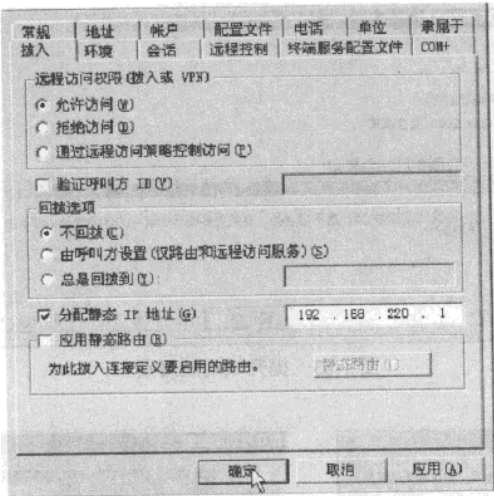


图 1-68 为高级 VPN 用户分配静态 IP 地址

首先在 ISA Server 管理控制台中，在“防火墙策略”中，禁用原来的“VPN 客户端访问策略”，如图 1-69 所示。

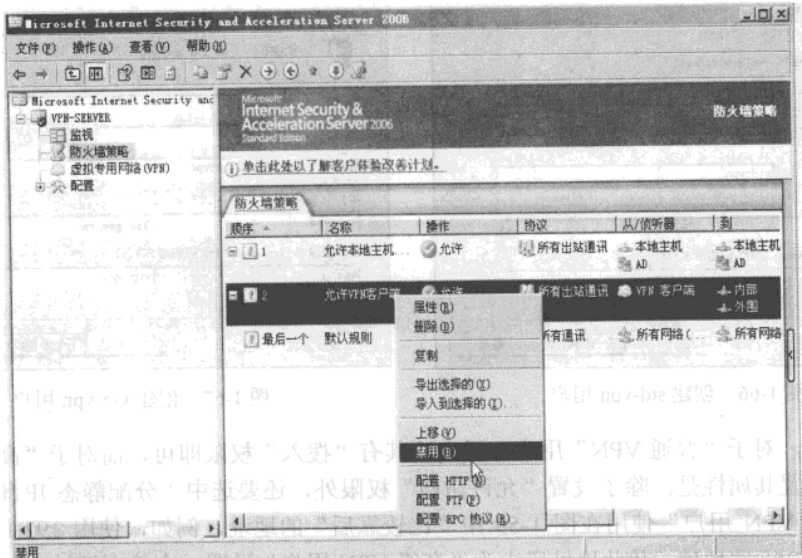


图 1-69 禁用原来的 VPN 访问策略

然后创建“标准 VPN 用户访问规则”，该规则允许 IP 地址为 192.168.200.1～192.168.219.255 的计算机访问指定的计算机，具体步骤如下。

第 1 步，新建访问规则，名称为“标准 VPN 用户访问规则”，如图 1-70 所示。

第 2 步，在“访问规则源”页中，单击“添加”按钮，在“网络实体”页中单击“新建→地址范围”（如图 1-71 所示），在“新建地址范围规则元素”对话框中，在“名称”文本框中输入“标准 VPN 地址范围”，指定地址范围为 192.168.200.1～192.168.219.255（如图 1-72

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示），然后创建“高级 VPN 地址范围”，地址范围为 192.168.220.1～192.168.220.255（如图 1-73 所示），然后到“网络实体”页，双击“标准 VPN 地址范围”，如图 1-74 所示。

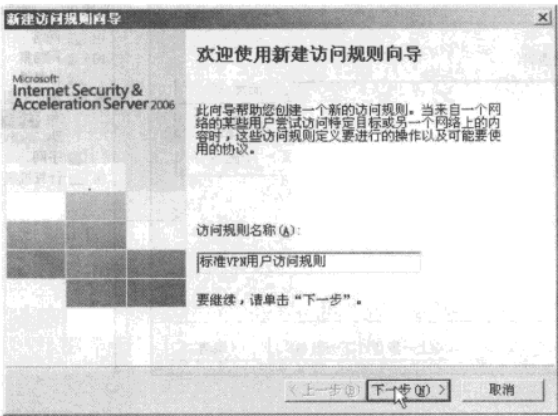


图 1-70 标准 VPN 用户访问规则

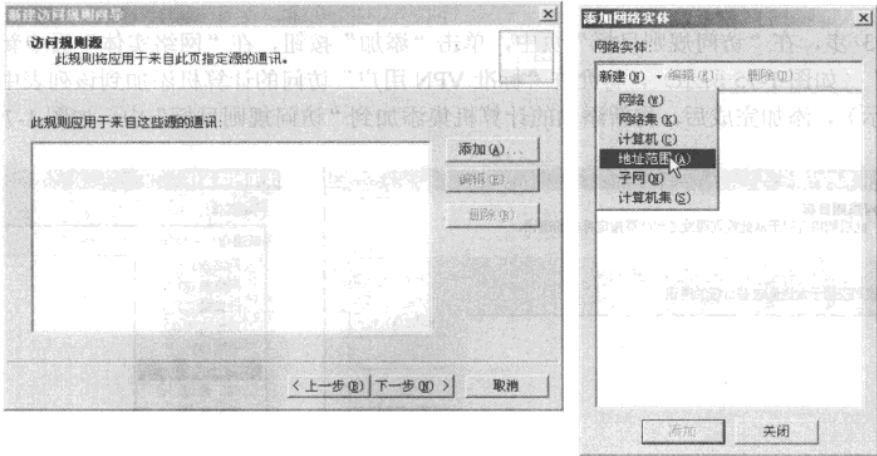


图 1-71 新建地址范围

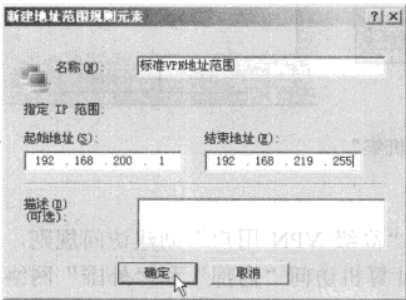


图 1-72 标准 VPN 地址范围

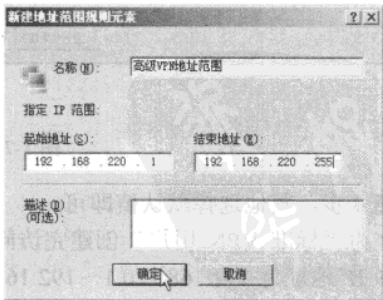


图 1-73 高级 VPN 地址范围

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

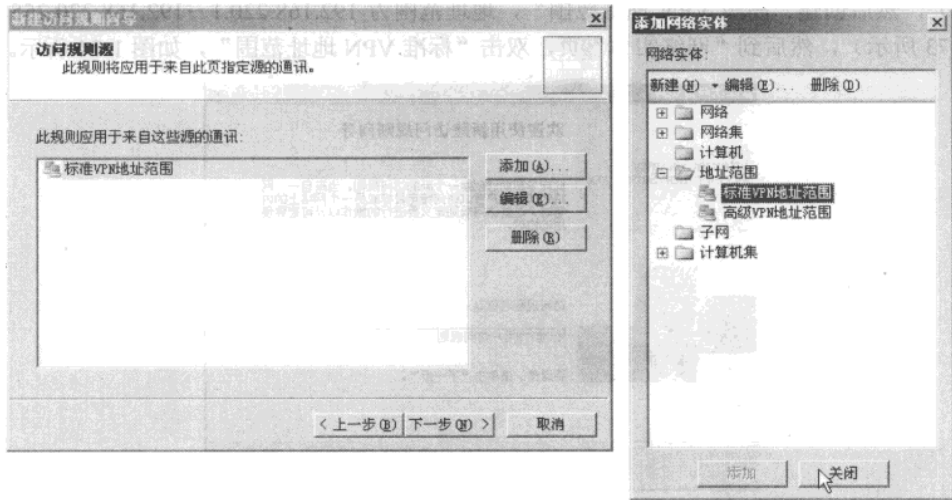


图 1-74 选择标准 VPN 地址范围

第 3 步，在“访问规则目标”页中，单击“添加”按钮，在“网络实体”页中新建“计算机集”（如图 1-75 所示），将允许“标准 VPN 用户”访问的计算机添加到该列表中（如图 1-76 所示），添加完成后，将新添加的计算机集添加到“访问规则目标”中，如图 1-77 所示。

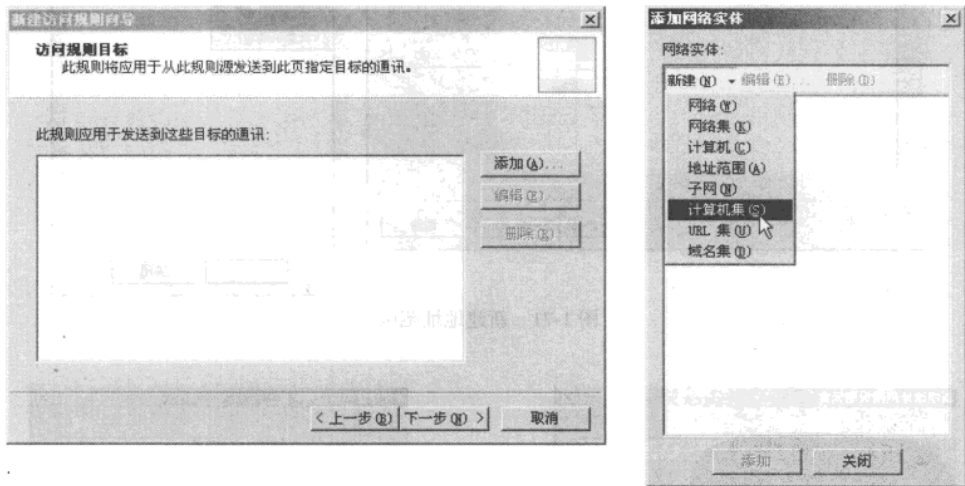


图 1-75 新建“计算机集”

第 4 步，其他选择默认值即可。

在为“标准 VPN 用户”创建完访问规则后，为“高级 VPN 用户”创建访问规则，该规则允许 IP 地址为 192.168.220.1~192.168.220.255 的计算机访问“内部”和“外围”网络，主要步骤如下。

第 1 步，访问规则名称为“高级 VPN 用户访问规则”，如图 1-78 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

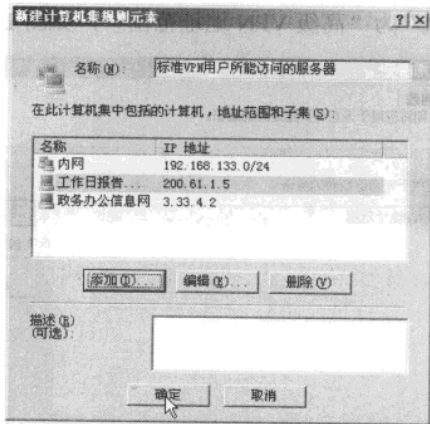


图 1-76 允许标准 VPN 用户访问的列表

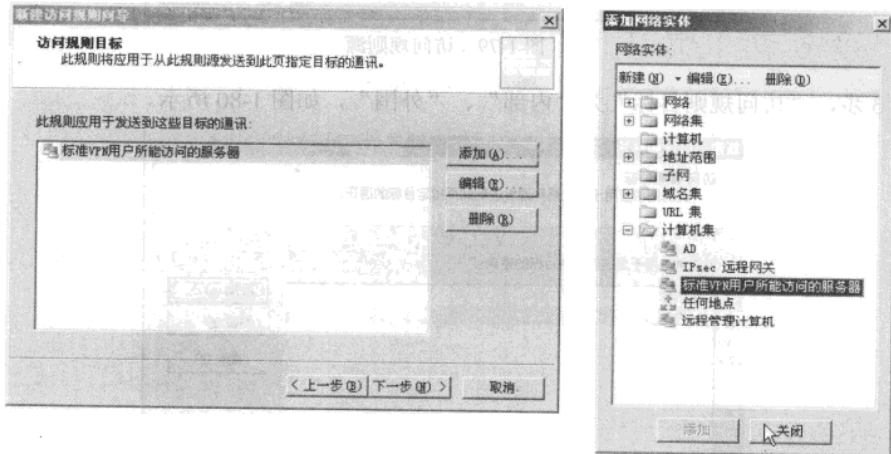


图 1-77 添加到访问规则目标中

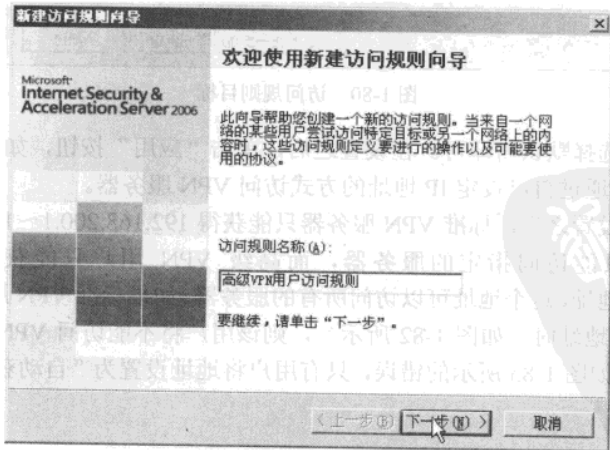


图 1-78 高级 VPN 用户访问规则

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 2 步，“访问规则源”为“高级 VPN 地址范围”，如图 1-79 所示。

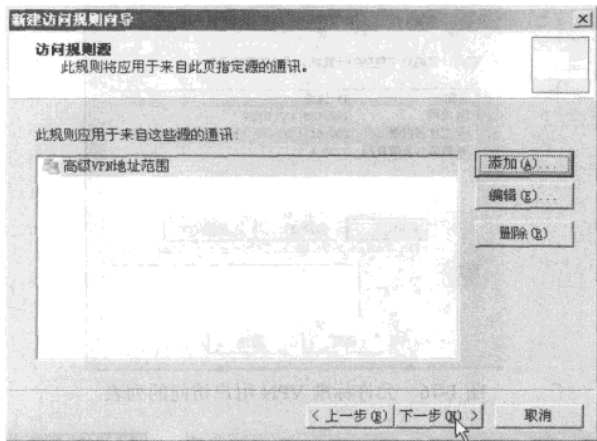


图 1-79 访问规则源

第 3 步，“访问规则目标”为“内部”、“外围”，如图 1-80 所示。

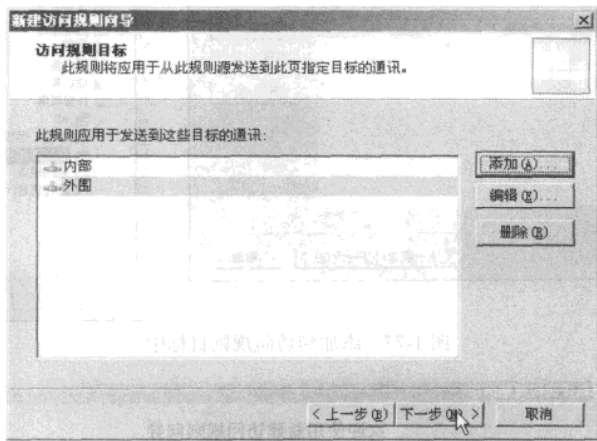


图 1-80 访问规则目标

第 4 步，其他选择默认值即可。在设置之后，单击“应用”按钮，如图 1-81 所示。

(4) 用户不能通过自己设定 IP 地址的方式访问 VPN 服务器。

在采用本节的设置之后，标准 VPN 服务器只能获得 192.168.200.1~192.168.4.250 之内的地址，这个地址只能访问指定的服务器，而高级 VPN 用户只能获得 192.168.220.1~192.168.220.255 的地址，这个地址可以访问所有的服务器。如果标准 VPN 服务器，尝试在 VPN 客户端自己设置 IP 地址时（如图 1-82 所示），则该用户将不能访问 VPN 服务器并且在拨号 VPN 服务器时出现如图 1-83 所示的错误，只有用户将地址设置为“自动获得 IP 地址”时，该用户才能使用。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

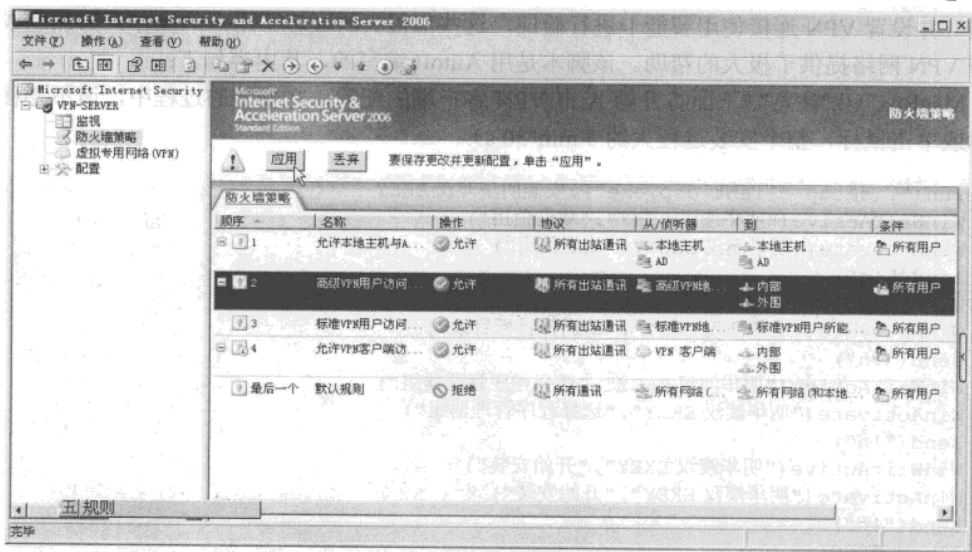


图 1-81 让设置生效

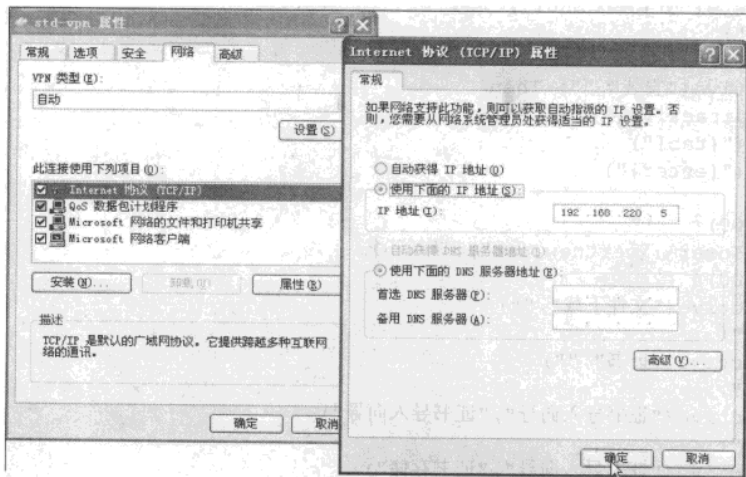


图 1-82 VPN 客户端自己设置 IP 地址

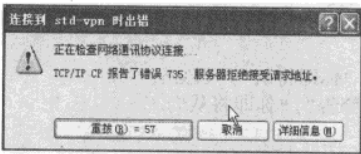


图 1-83 客户端自己设置地址后不能访问 VPN 服务器

7. 使用脚本安装驱动并配置证书、创建 VPN 连接

在给 A 市政府各部门、各乡镇部署 VPN 的时候，为了减轻用户的负担，我们制作了脚本，该脚本在执行过程中将“自动信任证书颁发机构”、“自动安装驱动程序”、“自动创建 VPN

网管天下 网管经验谈

连接”并设置 VPN 连接使用智能卡进行验证，这些都极大的减轻了用户的操作，为加速成功部署 VPN 网络提供了极大的帮助。该脚本是用 AutoIt 编写的，其内容如下：

MsgBox (0,"注意","下面将开始 A 市 VPN 客户端的配置，在安装的过程中，请不要移动鼠标或单击鼠标，整个安装过程大约 5 min"30 s)

```
run(".\setup_client_csp.exe");安装明华澳汉 EKEY
WinWaitActive("明华澳汉 EKEY","欢迎使用")
WinActivate("明华澳汉 EKEY","欢迎使用")
send("{!n}")
WinWaitActive("明华澳汉 EKEY","请选择目标目录")
WinActivate("明华澳汉 EKEY","请选择目标目录")
send("{!n}")
WinWaitActive("明华澳汉 EKEY","选择程序管理器组")
WinActivate("明华澳汉 EKEY","选择程序管理器组")
send("{!n}")
WinWaitActive("明华澳汉 EKEY","开始安装")
WinActivate("明华澳汉 EKEY","开始安装")
send("{!n}")
sleep(5000)
WinWaitActive("明华澳汉 EKEY","完成")
WinActivate("明华澳汉 EKEY","完成")
send("{!f}")
sleep(5000)
if winactive("安装","") Then
    winwaitactive("安装","")
    send("{tab}")
    send("{enter}")
endif
sleep(5000)
run("explorer .\certnew.cer");导入证书
sleep(3000)
WinWaitActive("文件下载","")
send("{!o}")
WinWaitActive("证书","")
send("{!i}")
WinWaitActive("证书导入向导","证书导入向导")
send("{!n}")
WinWaitActive("证书导入向导","证书存储")
send("{!n}")
WinWaitActive("证书导入向导","正在完成证书导入向导")
send("{ENTER}")
sleep(4000)
if WinActive("安全警告","你即将从") then
    winwaitactive("安全警告","你即将从")
    send("{!y}")
endif
WinWaitActive("证书导入向导","导入成功")
send("{ENTER}")
WinClose("证书","")
sleep(2000)
Run("control.exe netconnections");创建 VPN
WinWaitActive("网络连接","")
WinActivate("网络连接","")
```

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
send("!fn")
WinWaitActive("新建连接向导","")
WinActive("新建连接向导","")
send("!n")
WinWaitActive("新建连接向导","连接到 Internet")
WinActive("新建连接向导","连接到 Internet")
send("!on")
WinWaitActive("新建连接向导","虚拟专用网络连接")
WinActive("新建连接向导","虚拟专用网络连接")
send("!vn")
WinWaitActive("新建连接向导","公司名")
WinActive("新建连接向导","公司名")
send("!aShiVPN!n")
sleep(2000)
if WinActivate("新建连接向导","不拨初始连接") then send("!dn")
WinWaitActive("新建连接向导","主机名")
WinActive("新建连接向导","主机名")
send("!h10.10.10.30!n")
sleep(2000)
if WinActivate("新建连接向导","使用我的智能卡") then send("!un")
WinWaitActive("新建连接向导","正在完成新建连接向导")
WinActive("新建连接向导","正在完成新建连接向导")
send("!s")
send("{ENTER}")
sleep(3000)
if winactive("网络连接","") Then
    winwaitactive("网络连接","")
    send("{enter}")
EndIf
sleep(5000)
msgbox (0,"OK","安装完成",30)
```

如果要修改 VPN 服务器的地址，请将脚本中的“10.10.10.30”替换为实际的 VPN 服务器的地址即可。

在测试脚本无误后，将该脚本编译成可执行程序，最后一同提供给用户 3 个文件（如图 1-84 所示）：AutoIT 脚本可执行程序、驱动程序、根证书文件，将这 3 个文件提供给用户后，用户执行 AutoIT 的可执行程序（图中为 vpn-auto.exe），将自动完成上面的一系列操作。

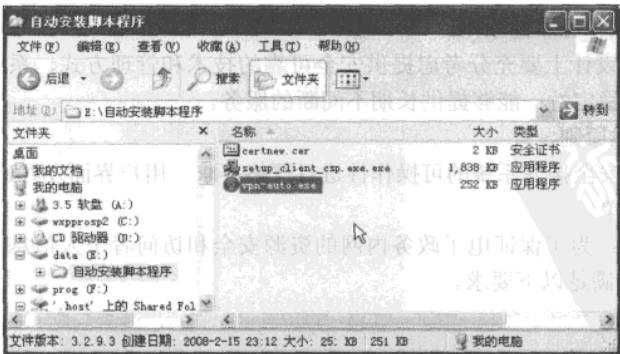


图 1-84 使用脚本完成安装

1.4.2 电子政务 VPN 应用案例分析

1. 客户背景

某市信息中心是正科级全额拨款事业单位，挂靠该市政府办公室，负责全市信息化建设的规划、指导和组织工作，主要承担该市区电子政务的建设和管理工作。目前，该市信息中心的内网上接直属地级市市委、市政府，下联市直 80 多个部门、14 个乡镇、2 个经济技术开发区。为方便市领导上 Internet 的需要，信息中心还向网通、电信各申请了 20 M Internet 带宽，通过双 WAN 口路由器，实现网通、电信双线路负载均衡。为了方便网上办公和网上审批工作，每个部门都建立了自己的局域网，预计全市办公内网的计算机保有量约 3 000 台以上，该市的信息化应用水平在其直属地级市各县市区中一直名列前茅。

2. 前景分析

以前，该市政府的电子政务内网是各单位向网通公司申请专线，通过网通公司在其核心交换机上划分 VLAN 来实现与其他网络隔离的，每年除需支付高额的线路租费外，也存在着网络安全的重大问题。

各单位除需建立内网支持网络办公以外，还需要建立外网，以获取更多的 Internet 信息和提供电子邮件、MSN、QQ 等交流工具，各单位对内、外网缺一不可。由于各单位的计算机有限，且不可能做到每人一机和内外网专机专用，这就使每个单位的内、外网有可能并到一起，使一台计算机即能上内网又同时上外网，即将内网线路和外网线路同时接到一台交换机上，并在终端上同时加入内、外网 IP 地址，即可实现一机上两网。这样，各单位都有可能成为内网的后门，内网随时有可能暴露在外网之中，其内网的安全性荡然无存。尽管有制度来约束工作人员，但一机上两网的便捷性还是让工作人员忘记了制度，而且这种上网方式也不易被发现，拔掉网线或关机，即便再好的网络监测设备也无济于事。为了解决这一问题，有针对性地定制了该市电子政务 VPN 应用解决方案。

（1） 受权许可性原则。

本原则一是保证在业务系统传输中业务数据的机密性和完整性，不能被非法或未授权用户获取和篡改；二是建立完善的用户和设备认证机制，确保非法用户和非法设备不能进入系统。

（2） 高可用性和可靠性原则。

本原则要求在设计上要充分考虑提供安全可靠的技术和管理方式，系统必须要保证其工作的高可靠性和高稳定性；能够提供长期不间断的服务。

（3） 易操作性原则。

本原则主要对安全接入系统的可操作性进行严格要求。用户界面友好，操作方便、简单；系统维护方便、简单。

技术实现要求：为了保证电子政务内网的资源安全和访问者个人信息的安全，访问的便捷，VPN 系统必需满足以下要求。

（1） 身份认证。

（2） 加密保护。

（3） 方便安全的管理。要求在管理上能有多种方式。提供本地网络管理、TELNET 管理，

网络方面 | 1

远程管理等多种管理方式，在以上方式中能对 VPN 安全策略、访问控制策略等进行调整。

(4) DHCP 支持。要求能给每一个接入 VPN 的用户动态分配一个内网 IP 地址，免除了各客户端的上网设置。

(5) 多种用户环境支持。支持专线宽带接入、ADSL 宽带接入，只要能够接入 Internet 的，都可以通过 VPN 接入内网。

(6) 本地网络和 VPN 网络智能判断。能根据客户的访问请求，自动选择使用客户本地连接还是使用 VPN 连接。

(7) 应用范围广。可在 VPN 用户与远程局域网之间应用多种业务。如：语音、图像和数据库等应用，也可通过共享等方式访问其他计算机资源。

(8) 由于内网中拥有数千名工作人员，因此对 VPN 设备的并发客户端性能要求达到 1 千个以上。

(9) 符合国家相关法律、标准和安全要求。各 VPN 设备必须符合我国的各项技术标准和标准。

(10) 系统可升级性。可以通过对 VPN 系统升级来适应新的网络应用或是 VPN 上相关协议或标准的升级。

3. 应用效果

经过改造，该市的电子政务内网不论是与信息中心在同一局域网的楼内单位，还是与信息中心不在同一局域网的楼外单位，均通过智能卡和数字证书通过 VPN 登录办公内网。不同级别的智能卡只能不同的系统，保证了什么级别的用户登录什么系统，确保了系统和信息资源的安全性和信息保密级别的有效性。通过 VPN 系统，可以了解到哪个用户在什么时间访问什么资源，确保了信息访问的可追溯性，从另一个方面，加强了对网内用户的规范操作，杜绝了从内部产生网络安全的隐患，VPN 系统确保了不论是在何时何地，只要通过 VPN 上内网，则外网强制断开，避免了一台计算机同时上两网的现象，同时也避免了办公系统暴露到外网的可能。由于 VPN 技术是通过外网建立加密隧道进入内网的，每个单位只解决外网线路即可，为各单位节约了大量的专线费用。同时，为移动办公创造了条件，只要手持智能卡，不论在哪，只要能上外网，就能进行网上办公。由于 VPN 技术的应用，越来越多的单位都将自己的业务搬到了网上，极大地推进了信息技术的应用，使该市的电子政务建设又上了一个新台阶。

1.5 网络实验方面经验

本节介绍了修改 MAC 地址的方法、虚拟局域网、百兆位至千兆位网络升级和局域网加速四个实验类型的应用，为企业网络出现的问题的解决提供参考。

1.5.1 修改 MAC 地址方法

MAC 地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。IP 地址与 MAC 地址在计算机里都是以二进制表示的，IP 地址是 32 位的，而 MAC 地址则是 48 位的。MAC 地址的长度为 48 位（6 个字节），通常表示为 12 个 16 进制数，每 2 个 16 进制数之间用冒号隔开，如：08:00:20:0A:8C:6D 就是一个 MAC 地址，其中前 6 位 16 进制数

网管天下 网管经验谈

08:00:20 代表网络硬件制造商的编号，它由 IEEE（电气与电子工程师协会）分配，而后 6 位 16 进制数 0A:8C:6D 代表该制造商所制造的某个网络产品（如网卡）的系列号。只要你不更改自己的 MAC 地址，那么你的 MAC 地址在世界上是唯一的。

（1）MAC 地址的作用。

IP 地址就如同一个职位，而 MAC 地址则好像是去应聘这个职位的人才，职位可以既可以让甲坐，也可以让乙坐，同样的道理一个结点的 IP 地址对于网卡是不做要求的，基本上什么样的厂家都可以用，也就是说 IP 地址与 MAC 地址并不存在着绑定关系。本身有的计算机流动性就比较强，正如同人才可以给不同的单位干活的道理一样的，人才的流动性是比较强的。职位和人才的对应关系就有点像是 IP 地址与 MAC 地址的对应关系。比如，如果一个网卡坏了，可以被更换，而无需取得一个新的 IP 地址。如果一个 IP 主机从一个网络移到另一个网络，可以给它一个新的 IP 地址，而无需换新的网卡。当然 MAC 地址除了仅仅只有这个功能还是不够的，就拿人类社会与网络进行类比，通过类比，我们就可以发现其中 MAC 地址的作用。

无论是局域网，还是广域网中的计算机之间的通信，最终都表现为将数据报从某种形式的链路上的初始结点出发，从一个结点传递到另一个结点，最终传送到目的结点。数据包在这些结点之间的移动都是由 ARP（Address Resolution Protocol：地址解析协议）负责将 IP 地址映射到 MAC 地址上来完成的。其实人类社会和网络也是类似的，试想在人际关系网络中，甲要捎个口信给丁，就会通过乙和丙中转一下，最后由丙转告给丁。在网络中，这个口信就好比是一个网络中的一个数据包。数据报在传送过程中会不断询问相邻结点的 MAC 地址，这个过程就好比是人类社会的口信传送过程。相信通过这两个例子，我们就可以进一步理解 MAC 地址的作用。

（2）与 MAC 地址相关的命令与软件。

在人类社会社交中，我们认识一个人往往只会知道他的姓名，而身份证号码在一般的人际交往中会被忽略。同样在网络中，我们往往只会知道同事或者网友的 IP 地址，并不会去过多地关心对方的 MAC 地址。要成长为网络高手，我们可以使用一些方法去了解对方的 MAC 地址。在这里介绍两种常用的方法，在 Windows 9x 中可用 WinIPcfg 获得，在 Windows 2000/XP 中可用 IPconfig -all 获得。

使用命令只能单条获得 MAC 地址，而且使用起来也是很麻烦的。对于网管人员，更希望有一款简单化操作的软件，我们可以利用“MAC 扫描器”远程批量获取 MAC 地址。它是用于批量获取远程计算机网卡物理地址的一款网络管理软件。该软件运行于网络（局域网、Internet 都可以）内的一台计算机上，即可监控整个网络的连接情况，实时检测各用户的 IP、MAC、主机名、用户名等并记录以供查询，可以由用户自己加以备注；能进行跨网段扫描，能和数据库中的 IP 和 MAC 地址进行比较，有修改 IP 的或使用虚假 MAC 地址的，都能报警。

（3）更改 MAC 地址。

一般 MAC 地址在网卡中是固定的，当然也有网络高手会想办法去修改自己的 MAC 地址。修改自己的 MAC 地址有两种方法，一种是硬件修改，另外一种软件修改。

硬件修改的方法就是直接对网卡进行操作，修改保存在网卡的 EPROM 里面的 MAC 地址，通过网卡生产厂家提供的修改程序可以更改存储器里的地址。那么什么叫做 EPROM 呢？EPROM 是电子学中一种存储器的专业术语，它是可擦写的，也就是说一张白纸你用钢笔写了

一遍以后就不能再用橡皮擦去了，而 EPROM 这张白纸用铅笔写后可以再擦去，可以反复改变其中数据的存储器。

软件修改的方法相对来说要简单得多，在 Windows 中修改的方法前面 1.1.2 节曾经介绍过，依次右击“网上邻居→属性→本地连接→属性→配置→高级→Network Address”的值里修改，如图 1-85 所示。

完成上述操作后重启就好了。一般网卡发出的包的 MAC 地址并不是网卡本身写上去的，而是应用程序提供的，只是在通常的实现中，应用程序先从网卡上得到 MAC 地址，每次发送的时候都用这个 MAC 作为源 MAC 而已，而注册表中的 MAC 地址是在 Windows 安装的时候从网卡中读入的，只要你的操作系统不重新安装应该问题不大。

（4）MAC 地址的应用。

平日身份证的作用并不是很大，但是到了有些关键时刻，身份证就是用来证明你的身份的。比如你要去银行提取现金，这时就要用到身份证。那么 MAC 地址与 IP 地址绑定就如同我们在日常生活中亲自携带自己的身份证去做重要事情一样的道理。有的时候，我们为了防止 IP 地址被盗用，就通过简单的交换机端口绑定（端口的 MAC 表使用静态表项），可以在每个交换机端口只连接一台主机的情况下防止修改 MAC 地址的盗用，如果是三层设备还可以提供：交换机端口/IP/MAC 三者的绑定，防止修改 MAC 的 IP 盗用。一般绑定 MAC 地址都是在交换机和路由器上配置的，是网管人员才能接触到的，对于一般电脑用户来说只要了解绑定的作用就行了。比如你在校园网中把自己的笔记本电脑换到另外一个宿舍就无法上网了，这个就是因为 MAC 地址与 IP 地址（端口）绑定引起的。

（5）MAC 地址涉及到的安全问题。

从上面的介绍可以知道，这种标识方式只是基于 MAC 地址的，如果有人能够更改 MAC 地址，就可以盗用 IP 免费上网了，目前网上针对小区宽带的盗用 MAC 地址免费上网方式就是基于此这种思路。如果想盗用别人的 IP 地址，除了 IP 地址还要知道对应的 MAC 地址。举个例子，获得局域网内某台主机的 MAC 地址，比如想得到局域网内名为 TARGET 主机的 MAC 地址，先用 PING 命令：PING TARGET，这样在我们主机上面的 ARP 表的缓存中就会留下目标地址和 MAC 映射的记录，然后通过 ARP A 命令来查询 ARP 表，这样就得到了指定主机的 MAC 地址。最后用 ARP -s IP 网卡 MAC 地址，命令把网关的 IP 地址和它的 MAC 地址映射起来就可以了。

ARP 原理：某计算机 A 要向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后就会进行数据传输。如果未找到，则广播 A 一个 ARP 请求报文（携带主机 A 的 IP 地址 Ia——物理地址 Pa），请求 IP 地址为 Ib 的主机 B 回答物理地址 Pb。网上所有主机包括 B 都收到 ARP 请求，但只有主机 B 识别自己的 IP 地址，于是向 A 主机发回一个 ARP 响应报文。其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，就会更新本地的 ARP 缓存。接着使用这个 MAC 地址发送数据（由网卡附加 MAC 地址）。因此，本地高速缓存的这个 ARP 表是本地网络流通的基础，而且这个缓存是动态的。ARP 表：为了回忆通信的速度，

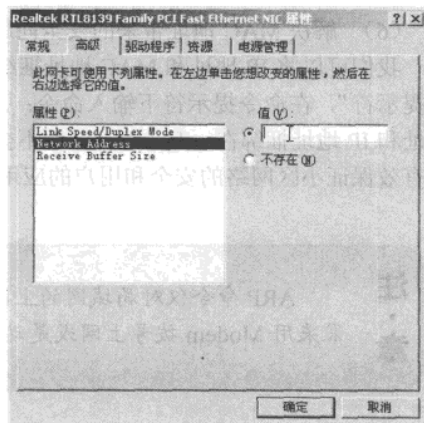


图 1-85 修改 MAC 地址

网管天下 网管经验谈

最近常用的 MAC 地址与 IP 的转换不用依靠交换机来进行，而是在本机上建立一个用来记录常用主机 IP-MAC 映射表，即 ARP 表。

（6）解决 MAC 地址带来的安全问题。

我们可以将 IP 地址和 MAC 地址捆绑起来来解决这个问题。进入“MS-DOS 方式”或“命令提示符”，在命令提示符下输入命令：ARP -s 10.88.56.72 00-10-5C-AD-72-E3，即可把 MAC 地址和 IP 地址捆绑在一起。这样，就不会出现 IP 地址被盗用而不能正常使用网络的情况，可以有效保证小区网络的安全和用户的应用。

注·意

ARP 命令仅对局域网的上网代理服务器有用，而且是针对静态 IP 地址，如果采用 Modem 拨号上网或是动态 IP 地址就不起作用。

1.5.2 虚拟局域网总结

1. VLAN 介绍

所谓 VLAN 是指处于不同物理位置的结点根据需要组成不同的逻辑子网，即一个 VLAN 就是一个逻辑广播域，它可以覆盖多个网络设备。VLAN 允许处于不同地理位置的网络用户加入到一个逻辑子网中，共享一个广播域。通过对 VLAN 的创建可以控制广播风暴的产生，从而提高交换式网络的整体性能和安全性。同一个 VLAN 中的端口可以接收 VLAN 中的广播包，别的 VLAN 中的端口则接收不到。

2. VLAN 在网络管理中的应用

假设以某集团公司为对象来介绍 VLAN 的应用。该集团下属公司多，业务种类多，根据业务发展需要，经过认真规划，将联网后的统一网络划分为 20 个 VLAN。划分原则为：集团本部以部门职能为单位进行 VLAN 划分，各下属公司以业务的不同来划分 VLAN，不同的 VLAN 具有不同的安全级别。其中生产用机及各种服务器所在的 VLAN 具有的安全级别较高。同时利用 Cisco 6509 自身的访问控制功能，设置访问列表对特定的 VLAN 用户进行保护，对特定的端口 135、445、1434 等进行控制，保证了整个网络中各个 VLAN 用户的安全隔离。VLAN 划分的有 4 种策略：基于端口的 VLAN 划分、基于 MAC 地址的 VLAN 划分、基于路由的 VLAN 划分、基于策略的 VLAN 划分。该集团采用的方式是基于端口的 VLAN 划分的方式。

基于端口的 VLAN 划分是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换机端口进行重新分配即可，不用考虑该端口所连接的设备。在交换机投入运行前就把它的物理端口根据需要划分给指定的 VLAN 并分配给用户。这种划分使网络管理员能够随时掌握网络的负载情况，有利于网络的优化使用，并具有较高的安全性，虽然在一定程度上增加了管理员的工作量。举例来说，集团下属公司分布在不同城市，但考虑到方便管理，这些公司的 OA 服务器均使用一个 VLAN 的 IP；对需要其他权限的 OA 服务器单独分配其他网段的 IP，

所有这些网络应用的实现均是依靠基于交换机端口 VLAN 的划分来实现的。

另一方面，对静态 VLAN 技术的应用（即基于端口的 VLAN 划分）来说，交换机不能分辨出被盗用 IP 地址的非法接入。一个用户盗用同一子网某特权用户的 IP 地址后就可以伪装成这个 VLAN 的特权用户，非法访问网络中的服务器，并造成 IP 地址的冲突。为了解决这个问题，就利用用户一般不会改变计算机 MAC 地址的特点，采用了对大部分用户的 IP 地址和 MAC 地址与交换机端口绑定的方法，弥补了静态 VLAN 的这一缺陷，有效地防止了这种情况的发生。满足了对不同 VLAN 设置不同访问权限。那么 VLAN 与 VLAN 之间又是如何实现相互间的访问呢？

在一般的二层交换机组成的网络中，VLAN 实现了网络流量的分割，不同的 VLAN 间是不能互相通信的。要实现 VLAN 间的通信必须借助：①路由器来实现；②三层交换机。其下属公司采用的是使用三层交换机的方式。利用三层交换机实现 VLAN 间通信，三层交换机是将第二层交换机和第三层路由器两者的优势有机而智能化地结合起来，可在各个层次提供线速性能。三层交换机内，分别设置了交换机模块和路由器模块；而内置的路由模块与交换模块类似，也使用 ASIC 硬件处理路由。因此，与传统的路由器相比，可以实现高速路由。并且，路由与交换模块是汇聚链接的，由于是内部连接，可以确保相当大的带宽。用三层交换机的路由功能来实现 VLAN 间的通信。

核心交换机选用 Cisco 6509 三层交换机，接入层交换机选择了 Cisco 3750 和 Cisco 2950 系列交换机，其中 Cisco 3750 交换机为带路由功能的三层交换机，用于数据流量较大的分局，而 Cisco 2950 为二层交换机，主要用于通过千兆光纤与中心交换机的直接连接，通过这样的连接方式，整个局域网就能很好的协同工作。VLAN 对于网络使用者来说是完全透明的，用户在使用中感觉不到与交换式网络有任何的差别，但对于网络管理人员则有很大的不同，因为这主要取决于 VLAN 的几点优势。

（1）控制广播风暴：网络管理必须解决因大量广播信息带来带宽消耗的问题。VLAN 作为一种网络分段技术，可将广播风暴限制在一个 VLAN 内部，避免影响其他网段。与传统局域网相比，VLAN 能够更加有效地利用带宽。在 VLAN 中，网络被逻辑地分割成广播域，由 VLAN 成员所发送的信息帧或数据包仅在 VLAN 内的成员之间传送，而不是向网上的所有工作站发送。这样可减少主干网的流量，提高网络速度。

（2）增强网络的安全性：共享式 LAN 上的广播必然会产生安全性问题，因为网络上的所有用户都能监测到流经的业务，用户只要插入任一活动端口就可访问网段上的广播包。采用 VLAN 提供的安全机制，可以限制特定用户的访问，控制广播组的大小和位置，甚至锁定网络成员的 MAC 地址。这样就限制了未经安全许可的用户和网络成员对网络的使用。

（3）增强网络管理：采用 VLAN 技术，使用 VLAN 管理程序可对整个网络进行集中管理，能够更容易地实现网络的管理性。用户可以根据业务需要快速组建和调整 VLAN。当链路拥挤时，利用管理程序能够重新分配业务。管理程序还能够提供有关工作组的业务量、广播行为以及统计特性等的详尽报告。对于网络管理员来说，所有这些网络配置和管理工作都是透明的。VLAN 变动时，用户无需了解网络的接线情况和协议是如何重新设置的。另外在使用 VLAN 划分后，也较好的解决了客户机随意使用 IP 地址的问题，因为某台计算机是属于某个特定的 VLAN 的，如果设置其他 VLAN 的 IP 地址，则是不能接入局域网的。

1.5.3 百兆位至千兆位的网络升级经验

随着百兆位连接到桌面的实现，以及网络多媒体应用的增多，对交换机之间以及交换机到服务器之间带宽的要求越来越高，原有带宽已经成为制约网络传输的瓶颈。于是，将主干网络提升至千兆位以太网，就被列入了各大、中型网络的规划中。

(1) 千兆位标准与传输介质。

千兆位以太网所使用的传输介质主要为单模光纤、多模光纤以及非屏蔽双绞线。目前，千兆位以太网标准有两个，一是 IEEE 802.3z（定义 1000Base-LX、1000Base-SX、1000Base-LH 和 1000Base-ZX），二是 IEEE 802.3ab（定义 1000Base-T），它们分别用于规范在光纤和非屏蔽线缆上传输千兆位信号。

(2) 升级方案。

只须将网络中心交换机由原来的快速以太网交换机更换为千兆位以太网交换机，即可将网络主干提升至千兆位。然后就是将交换机与服务器之间的连接升级至千兆位。如果资金允许，可进一步提升骨干交换机与工作组交换机之间的连接，从而搭建真正的千兆位网络。

1. 升级网络骨干

准备将快速以太网升级至千兆位以太网时，首先应当考虑将中心交换机升级为千兆位以太网交换机（如 Cisco Catalyst 4000 系列或 Catalyst 6500 系列），提供足够数量的千兆位端口。然后，升级骨干交换机，使骨干交换机拥有千兆位端口（如 Cisco Catalyst 3550G 系列或 Catalyst 2950G 系列），从而实现与中心交换机的千兆位互联，如图 1-86 所示。

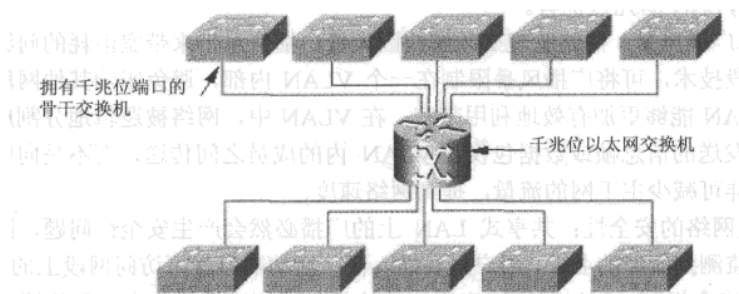


图 1-86 交换机的千兆位互联

根据网络需求的不同，骨干交换机既可以全部采用千兆位端口（如 Cisco Catalyst 3550-12G），也可以采用“千兆位端口+快速以太网端口”（如 Cisco Catalyst 3550G-24-EMI）。

注：
意

在局域网中，80%的访问是针对服务器的，也就是说，对服务器的访问占绝大多数，而服务器通常都位于中心交换机附近，所以，绝大部分数据流量需要依靠网络骨干进行传输。即使是千兆位连接有时也不免捉襟见肘。必要的时候，不妨采用光纤聚合技术，即将多个千兆位连接绑定在一起，作为一个连接使用，从而成倍地提高骨干连接的带宽，达到 2 Gbps 或者更高。

2. 升级网络服务器

当网络骨干升级至千兆位后，服务器与网络的连接将成为数据传输瓶颈。如果服务器仍然采用原有的 100 Mbps，将无法适应网络升级后的访问需求。所以，必须将服务器与交换机的连接升级至 1000 Mbps。

超五类双绞线和六类双绞线都支持千兆位连接，而且双绞线设备的造价相对低廉，因此，如果交换机提供有 1000Base-T 端口，应当尽量为服务器选择双绞线端口的网卡，以节约投资。

注意 单一服务器往往难以胜任繁重的网络访问需求，因此，还应当采用服务器集群技术或负载均衡技术，将多个服务器有机地组织在一起，既可分担繁重的网络服务任务，又可实现服务器的冗余。

1.5.4 局域网加速方法小结

我们无时无刻不与局域网在打着交道，提供更快更稳定的局域网访问一直是我们的追求。除了购买更好的硬件外，只要我们稍做一些设置，并注意一些技巧，也可以得到更快的访问速度。

(1) 去掉无关的选项。

在 Windows XP 中，双击“控制面板”中的“文件夹选项”图标，再单击“查看”标签，然后将鼠标指针滚动至窗口的最下方，可以看到有一个“自动搜索网络文件夹和打印机”选项，默认是选中的，将它去掉如图 1-87 所示。这样，当我们打印时，Windows XP 不会自作主张去寻找局域网上的打印机并安装驱动程序，以防止不经意将机密文档打到别的部门打印机上而自己却还找不到。同时，将此项去掉后，当我们通过“网上邻居”来访问局域网计算机时时，它不会自动查找其上的共享文件夹，这样才会提升一些速度。

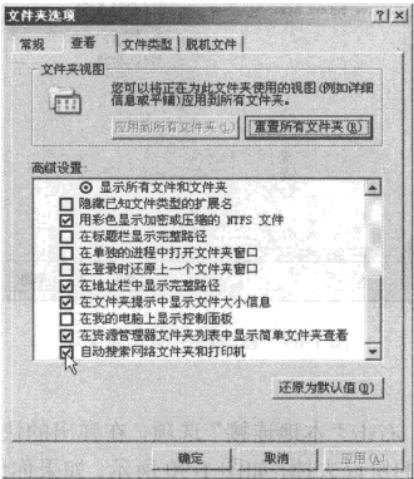


图 1-87 去掉“自动搜索网络文件夹和打印机”选项

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

(2) 将网卡调至全速。

按下 Win+Pause/Break 组合键，切换到“硬件”选项卡，再单击“设备管理器”按钮，从而打开“设备管理器”窗口，选择“网络适配器”选项，如图 1-88 所示。双击“Realtek RTL8139.Family PCI Fast Ethernet NIC”打开对话框，切换到“高级”选项卡，选中 Link Speed/Duplex Mode（连接速度/双工模式），再在“值”下选择 100 Full Mode，如图 1-89 所示。这样可以让网卡调至全速。当然，如果你使用的是无线网络，则将其调至最高速即可。

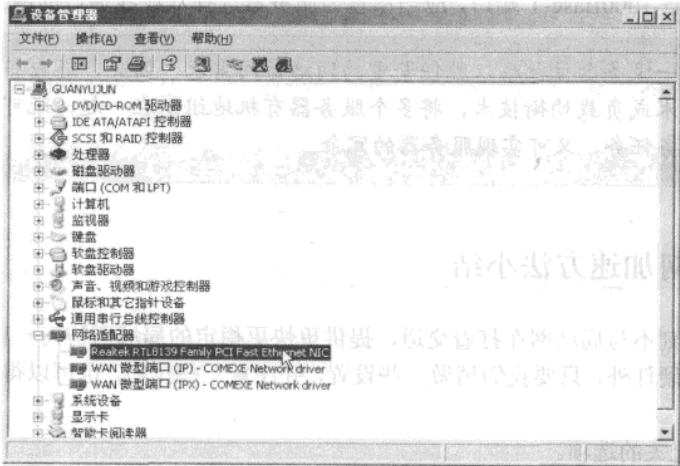


图 1-88 选择网络适配器

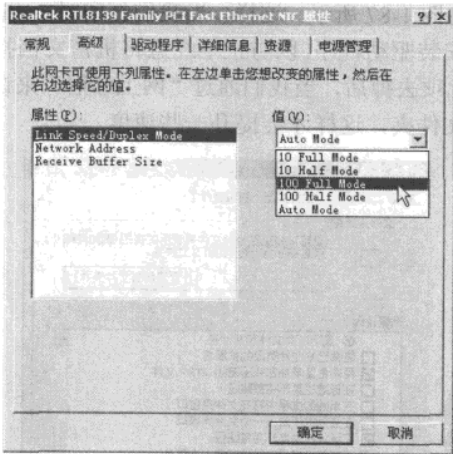


图 1-89 修改网卡模式为全速

(3) 去掉无关的协议。

打开“网络连接”窗口，右击“本地连接”选项，在弹出的快捷菜单中选择“属性”命令，然后在打开窗口中将不需要的协议去掉，如图 1-90 所示。如果你使用 Windows 98，则“TCP/IP-拨号适配器”、“Microsoft 友好登录”、“Microsoft 虚拟专用网络适配器”、“IPX/SPX 兼容协议”

等都可以去掉，因为这些组件平时不怎么用到，如果选中时，反而会影响工作站正常上网和浏览。

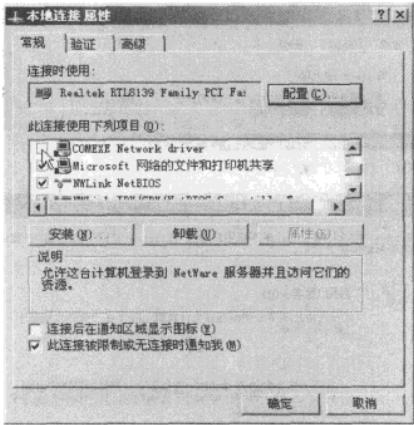


图 1-90 去掉不常用协议

(4) 自动登录局域网。

如果你每天都都需要访问某个共享文件夹，不需要按部就班地双击“网上邻居”，然后找到服务器，双击后输入用户名和密码再访问。比如，你要访问一个名为 server 的电脑，用户名为 user，密码是 8888。则只要写一个 bat 文件，在其中输入如下语句：net use serverIPC\$ "8888" /user:"user"，如图 1-91 所示。接着把该 bat 文件拖放到“开始”→“程序”→“启动”组中，这样一开机，系统就会以 user 为用户名，8888 为密码登录 server 计算机，这样你在任何地方访问它上面的共享文件夹则无需再输入用户名和密码了。

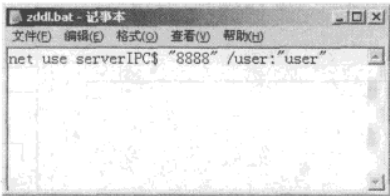


图 1-91 “自动登录”批处理命令

(5) 取消防火墙。

如果你启用了 Windows XP 中防火墙，且共享了驱动器，那有可能别人无法在“网络邻居”中浏览共享驱动器，这时可以右击“本地连接”选项，在弹出的快捷菜单中选择“属性”命令，切换到“高级”选项卡，单击“设置”按钮，打开如图 1-92 所示的窗口中选中“关闭（不推荐）”单选按钮即可。因为我们的局域网计算机本身就接在路由器上，可以考虑在上面设置防火墙。这样局域网内的计算机不会受到外界的攻击，局域网内的计算机访问也会快一些。

(6) 取消缓存设置。

在计算机上右击某文件夹，在弹出的快捷菜单中选择“共享和安全”选项，单击对话框下方的“缓存”按钮，再在打开的对话框中取消“允许在这个共享文件夹中缓存文件”复选框，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

如图 1-93 所示。这样当我们的共享文件夹下的文件非常多时，别人访问此共享文件夹加速会明显。如果不这样设置，可能很长时间无法打开此文件夹下的文件，而且有可能会让系统死机。

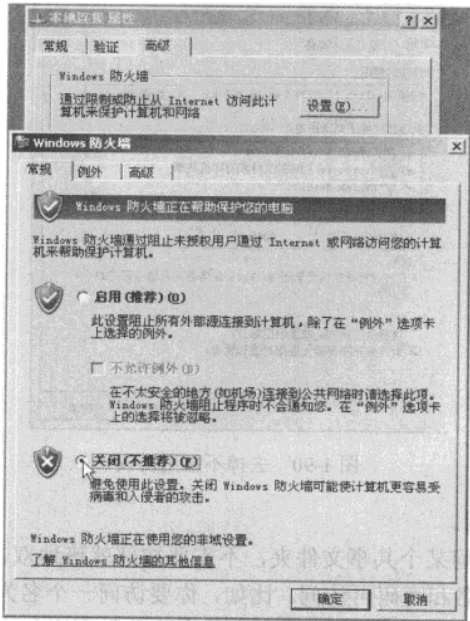


图 1-92 关闭防火墙

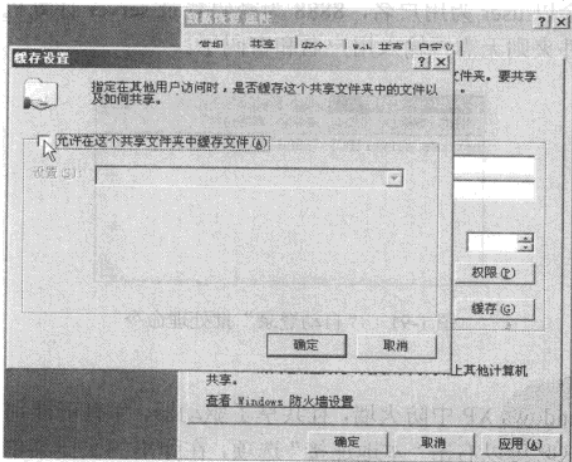


图 1-93 取消“允许在这个共享文件夹中缓存文件”复选框

(7) 可以考虑千兆位网卡和安装 64 位系统。

如果拥有千兆位网卡和 64 位的计算机，建议安装 64 位 Windows，据权威机构测试，它的局域网速度访问速度有明显的提升。

第2章 安全方面

现在计算机成了企业不可缺少的一种工具，不少企业也选择了在网络这个无形的市场来大展宏图。然而，在如今的企业局域网、电子商务等新事物出现之际，如何保证自己的计算机和网络的安全成为网络管理和维护的核心任务。

本章通过介绍计算机安全的一些基础知识，使初级网络管理员了解网络安全的重要性和如何防止自己的计算机出现安全方面的问题。详细介绍了一些日常的杀毒技巧和杀毒的小经验及如何维护数据的安全，当数据安全受到威胁和破坏时怎样用有效的方法来恢复数据。

2.1 计算机安全基础经验

本节将介绍预防计算机中毒的经验，以及在日常维护中如何通过 net 命令来检测网络的安全性。这些都是保证计算机安全的基本注意事项和技巧，日常维护中不仅要保证网络的安全，而且要在计算机中毒以后尽快的做出相应的处理，减小病毒对网络的危害。

2.1.1 如何保护计算机不中病毒的经验总结

对于网络管理员来说最常见的问题就是员工的计算机中毒了。大部分时候问题都不会太大，可有时因为一台计算机中毒了，就要花上两三个小时的时间来对付它，更可怕的是因为这一台计算机而使整个内部网络都受到攻击和影响。所以完全有必要做一些阻止类似事情发生的工作，加强防范意识。在本节中就介绍一些加强防范意识方面的经验。

(1) 保持获取信息。你是否知道几乎每天都有病毒和安全警告出现？通过把我们的安全与修复主页加入收藏夹来获取最新爆发的病毒。

(2) 如果你的计算机上没有安装病毒防护软件，你最好还是安装一个。如果你是一个家庭或者个人用户，下载任何一个排名最佳的程序都相当容易，而且可以按照安装向导进行操作。如果你在一个网络中，首先咨询你的网络管理员。

(3) 如果你刚好是第一次启动防病毒软件，最好让它扫描一下你的整个系统。干净并且无病毒问题地启动你的计算机是很好的一件事情。通常，防病毒程序都能够设置成在计算机每次启动时扫描系统或者在定期计划的基础上运行。一些程序还可以在你连接到 Internet 上时在后台扫描系统。定期扫描系统是否感染有病毒，最好成为你的习惯。

(4) 既然你安装了病毒防护软件，就应该确保它是最新的。一些防病毒程序带有自动连接到 Internet 上的功能，并且只要软件厂商发现了一种新的威胁就会添加新的病毒探测代码。你还可以在此扫描系统查找最新的安全更新文件。

(5) 有些附件极有可能带有计算机病毒或是黑客程序，轻易运行，很可能带来不可预测的结果。对于认识的朋友和陌生人发过来的电子邮件中的可执行程序附件都必须检查，确定无异后才可使用。

网管天下 网管经验谈

(6) 对方发送过来的电子邮件及相关附件的文档，首先要用“另存为...”命令（“Save As...”）保存到本地硬盘，待用查杀计算机病毒软件检查无毒后才可以打开使用。如果用鼠标直接单击两下 DOC、XLS 等附件文档，会自动启用 Word 或 Excel，如果附件中有计算机病毒则会立刻传染；如有“是否启用宏”的提示，那绝对不要轻易打开，否则极有可能传染上电子邮件计算机病毒。

(7) 对于文件扩展名很怪的附件，或者是带有脚本文件如*.VBS、*.SHS 等的附件，千万不要直接打开，一般可以删除包含这些附件的电子邮件，以保证计算机系统不受计算机病毒的侵害。

(8) 如果是使用 Outlook 作为收发电子邮件软件时，应当进行一些必要的设置。选择“工具”菜单中的“选项”命令，在“安全”中设置“附件的安全性”为“高”；在“其他”中单击“高级选项”按钮，单击“加载项管理器”按钮，不选中“服务器脚本运行”；最后单击“确定”按钮保存设置。

(9) 如果是使用 Outlook Express 作为收发电子邮件软件时，也应当进行一些必要的设置。选择“工具”菜单中的“选项”命令，在“阅读”中不选中“在预览窗格中自动显示新闻邮件”和“自动显示新闻邮件中的图片附件”。这样可以防止有些电子邮件计算机病毒利用 Outlook Express 的默认设置自动运行，破坏系统。

(10) 对于自己往外传送的附件，也一定要仔细检查，确定无毒后，才可发送。虽然电子邮件计算机病毒相当可怕，只要防护得当，还是完全可以避免传染上计算机病毒的，仍可放心使用。

在如今网络高度发达的时期，病毒是防不胜防的，只有筑好自己计算机上的防火墙和养成良好的上网习惯，才能把危害降到最低。当然了，这些经验网管员都知道，不过要是把它们总结到一块，再通过有效途径传给普通工作人员，这样从某种程度上会使网管员的工作事半功倍。

2.1.2 使用 Net 命令检测网络安全的小经验

作为网管员不应该只会借助一些软件工具来进行网络安全检测，其实在进行网络安全检测的过程中，各种 DOS 命令往往是能够找出蛛丝马迹最得心应手的工具。这样就不必担心软件有问题。本节就介绍一下比较实用的三条 net 命令来实现对网络的安全检测。

(1) 查看网络连接状态。

一般来说，安全主要是针对连接在网络上的计算机而言的。单机用户的安全问题比较少。而对于连接到网络上的计算机而言，最基本的就是对网络连接进行检测。因为不论是病毒，还是木马、黑客入侵等都是通过网络来连接的。

方法是在“运行”窗口中输入“CMD”，按 Enter 键打开命令提示符窗口，然后输入“netstat -an”命令，如图 2-1 所示，实现查看所有与本机建立的连接功能。

其中 Proto 部分表示连接方式，Local Address 是本地连接地址和端口，而 Foreign Address 则是对方的地址和端口，State 是当前端口的状态。看懂了这些信息后，读者就可以判断是否有异常的连接，如果有，则需要断开网络进行进一步的处理。

(2) 查看服务运行状态。

计算机的各项功能一般都是与其开放的服务相对应的。因此很多入侵者在进入计算机后

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

会开放各种服务，由此可见检测当前系统正在运行的服务是很有必要的。

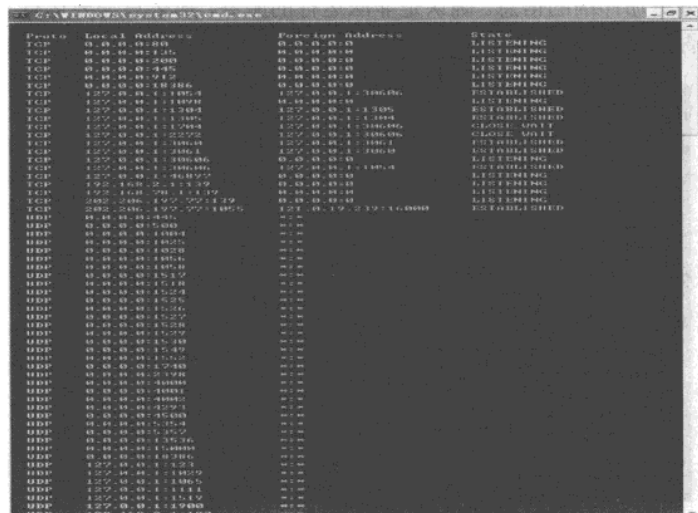


图 2-1 查看与本机的连接

方法是在命令提示符下输入“net start”命令，如图 2-2 所示，实现查看系统提示“已经启动以下 Windows 服务”的功能。



图 2-2 查看服务启动情况

网管天下 网管经验谈

然后从其列表中查看是否有不明服务在运行。如果有，则可以继续输入“net start 服务名”来查看有关该服务更加详细的信息。确认是非法运行的服务，那么只需要运行“net stop server”命令，在询问是否继续操作时，按“Y”键进行确认，如图 2-3 所示，实现停止此服务功能。

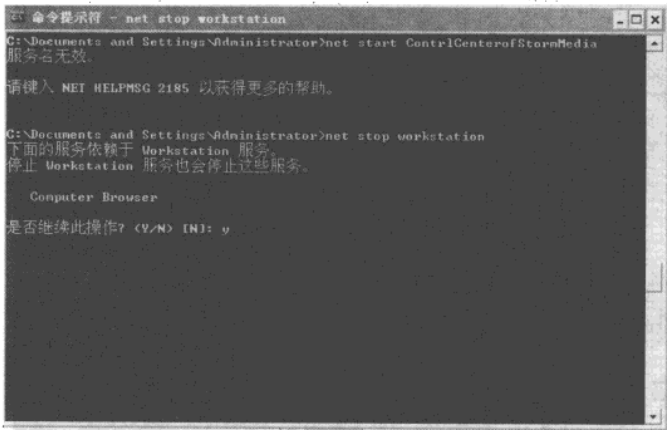


图 2-3 停止可疑服务

(3) 查看账户信息。

很多入侵者在突破防线后，一般都会建立相应的账户，以方便下次继续侵入。对此，我们可以在命令提示符下输入“net user”命令，如图 2-4 所示，实现显示当前系统中已经创建的所有账户名称功能。

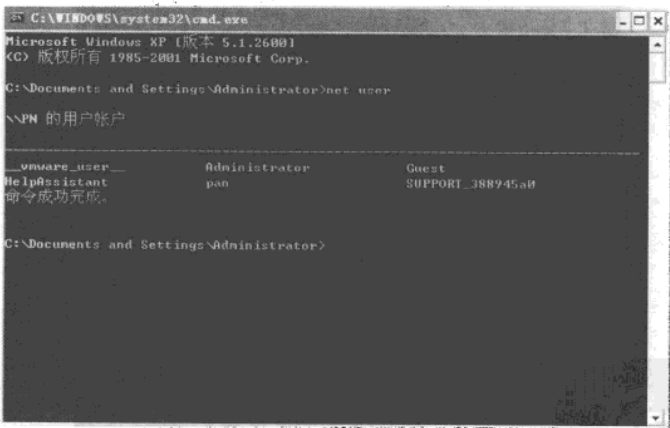


图 2-4 查看所有用户

如果发现不是自己创建的账户，那么则需要运行“net user 账户名称”命令，如图 2-5 所示，实现查看其拥有的权限的功能。

如果该用户属于 Administrators 等权限比较高的组的，那么可以确认该账户是黑客非法创建的，赶紧使用“net user 账户名称 /del”命令，如图 2-6 所示，实现删除该账户的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

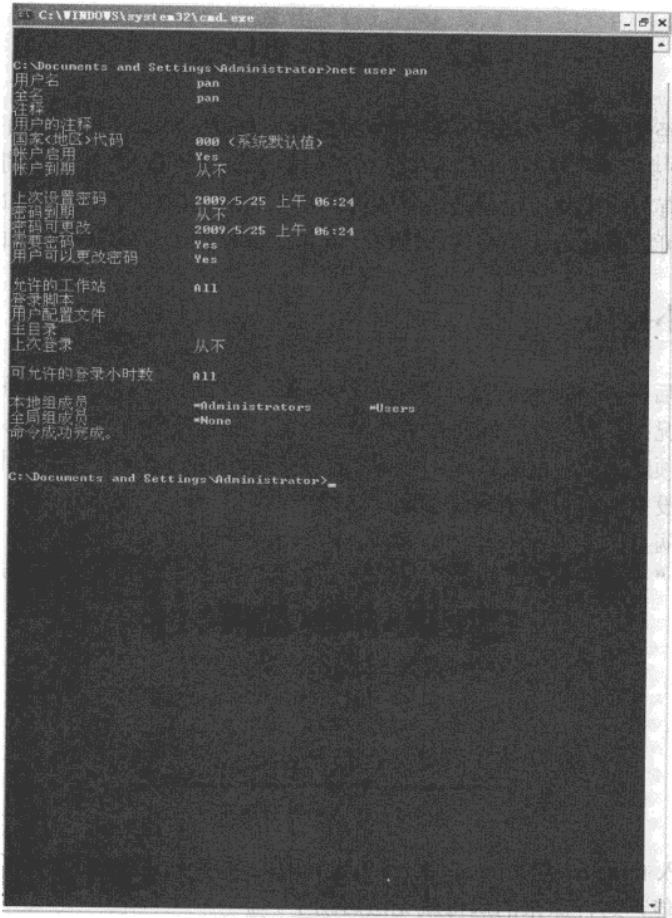


图 2-5 查看可疑账户的详细信息



图 2-6 删除可疑账户

2.2 杀毒经典经验

当计算机已经受到病毒的感染后，作为网络管理员要立即做出反应，在第一时间将病毒消灭，这就需要一些常用的技巧和日常生活中积累的一些小经验。在处理病毒的过程中当然还要借助一些比较有力的工具，也就是杀毒软件。在本节的 2.2.2 节中介绍了 NOD32 的客户端部署经验。希望可以借此迅速的将客户端统一部署杀毒软件，对病毒进行全面的清理。

2.2.1 杀毒小技巧

计算机中毒后，许多朋友会打开“进程管理器”，将几个不太熟悉的程序关闭掉，但有时会碰到这种情况：关掉一个，再去关闭另外一个时，刚才关闭的那个马上又运行了，再从注册表里先把启动项删除后，重启试试，刚删除的那些启动项又还原了。由于计算机只安装了一个操作系统，也没办法在另一个系统下删除这些病毒。上网下载专杀工具后，仍然不能杀掉。如此翻来覆去，病毒未杀掉，人却濒临崩溃。本节将介绍如何应对这种状况。

第 1 步，在“开始→运行”中输入 cmd，如图 2-7 所示，打开“命令提示符”窗口。

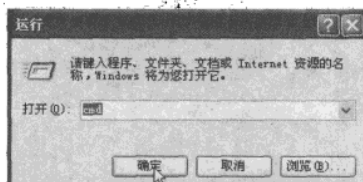


图 2-7 进入命令提示符

第 2 步，输入 `ftype exefile=notepad.exe %1`，如图 2-8 所示，实现将所有的 EXE 文件用“记事本”打开的功能，这样原来的病毒就无法启动了。

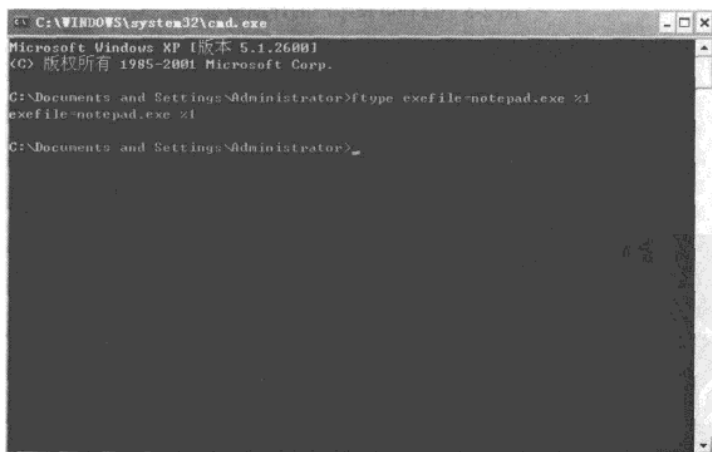


图 2-8 将 EXE 文件用“记事本”打开

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安全方面 | 2

第 3 步，重启计算机，你会看见打开了许多“记事本”，如图 2-9 所示。当然，这其中不仅有病毒文件，还有一些原来的系统文件，比如：输入法程序。

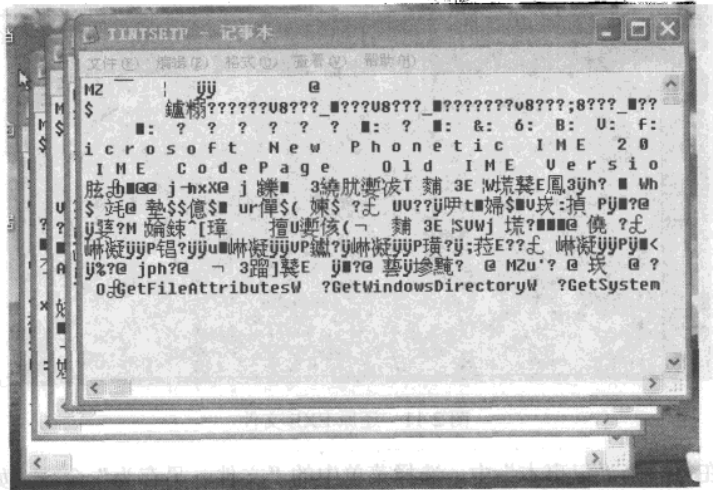


图 2-9 重启后自启动文件用记事本打开

第 4 步，右击任何文件，在弹出的快捷菜单中选择“打开方式”命令，然后单击“浏览”按钮，转到 WindowsSystem32 下，选择 cmd.exe 选项，如图 2-10 所示，实现再次打开“命令提示符”窗口的功能。



图 2-10 重新打开命令提示符窗口

第 5 步，运行 `ftype exefile=%1 %*`，如图 2-11 所示，将所有的 EXE 文件关联还原。现在运行杀毒软件或直接改回注册表，就可以杀掉病毒了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

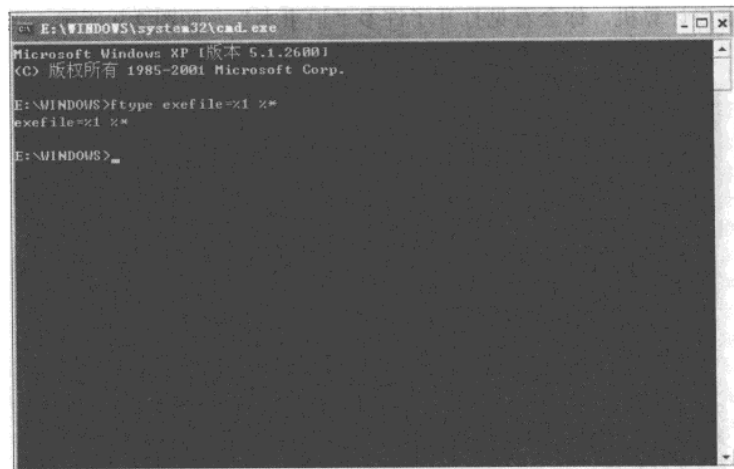


图 2-11 还原 EXE 文件

第 6 步，在每一个“记事本”中，选择菜单中的“文件→另存为”命令，如图 2-12 所示，实现查看路径和文件名的功能。找到病毒文件，手动删除即可，但得小心，必须确定那是病毒才能删除。建议将这些文件改名并记下，重启后如果没有病毒做怪，也没有系统问题，再进行删除。

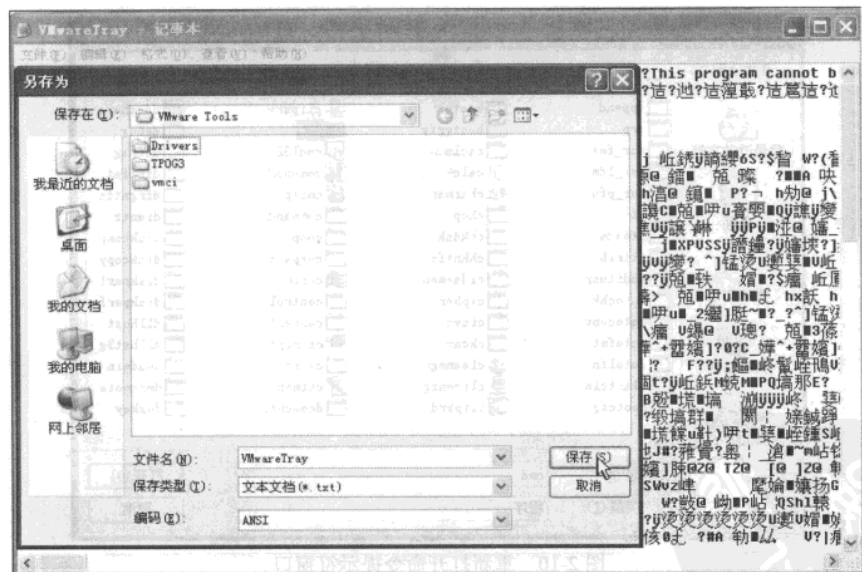


图 2-12 查找病毒文件

说·明

在 Windows 中，Ftype 命令用来显示及修改不同扩展名文件所关联的打开程序。相当于在注册表编辑器中修改“HKEY_CLASSES_ROOT”项下的部分内容。Ftype 的基本使用格式为：Ftype [文件类型]=[打开方式/程序]。比如：像上例中的 ftype exefile=notepad.exe %1，表示将所有文件类型为 EXE（exefile 表示为 EXE 类型文件）的文件都通过“记事本”程序打开，后面的 %1 表示要打开的程序本身（就是双击时的那个程序）。ftype exefile=%1 %*则表示所有 EXE 文件本身直接运行（EXE 可以直接运行，所以用表示程序本身的 %1 即可），后面的 %*则表示程序命令后带的所有参数（这就是为什么 EXE 文件可以带参数运行的原因）。

2.2.2 NOD32 3.0 客户端部署经验

NOD32 是一款不错的杀毒软件，以其极低的资源占用率、高效的查搜病毒能力，加上其多平台（Linux、Windows 等）支持能力，一直是广大网管的最优选择。

ESET 为企业用户提供了多种工具，用于在企业网络中部署 NOD32 3.0，例如，NOD32 3.0 的“远程管理工具”、“ESET 配置编辑器”，可以让管理员对 NOD32 3.0 的每个选项进行定制。例如，设置升级服务器的地址、远程管理服务器的地址、查杀病毒的等级等，如图 2-13 和图 2-14 所示。图 2-13 是 NOD32 3.0 的设置页，图 2-14 是 ESET 配置编辑器中对应图 2-13 的设置页。

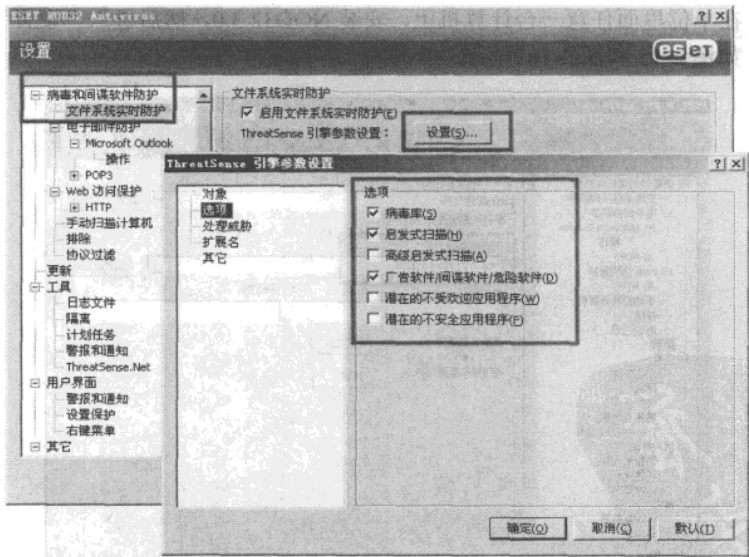


图 2-13 NOD32 “文件系统实时防护”设置界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

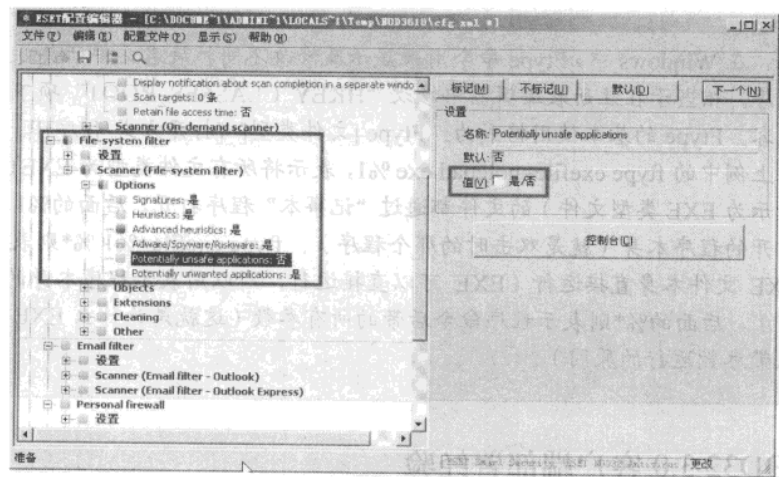


图 2-14 配置管理器

虽然使用 ESET 配置编辑器，可以定制 NOD32 3.0 的每一个选项，但该工具选项众多，很不容易理解里面的每个选项。另外，在使用 ESET 提供的“远程管理工具”时，最后生成的 NOD32 的安装程序，在安装的时候，还需要用户交互，这增加了用户的负担。

在本节作者将为读者介绍一个简单的方法：不需要 ESET 配置编辑器，也不需要 ESET 的“远程管理工具”，自己动手定制 NOD32 的安装程序，以及 NOD32 在安装后的每一个选项，并且最后生成的安装程序是“全自动的”，不需要用户交互就可以完成安装设置，下面介绍步骤。

第 1 步，在单位里面任意一台计算机上，安装 NOD32 3.0，然后进入“设置”页面，设置每一个选项，如图 2-15 和图 2-16 所示。

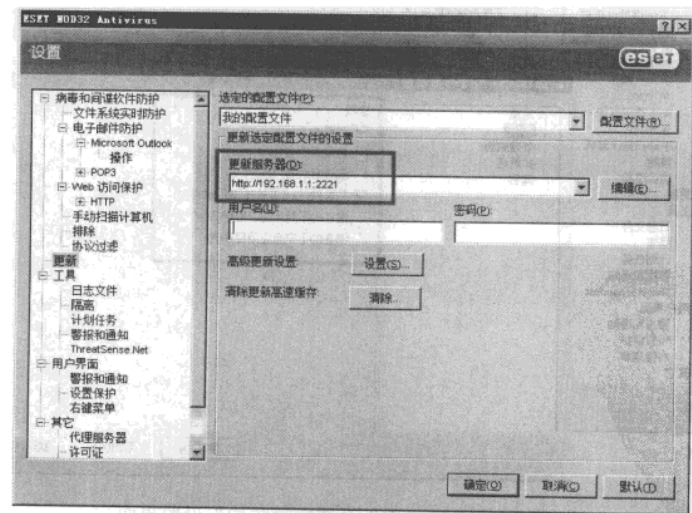


图 2-15 指定内部升级服务器地址

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

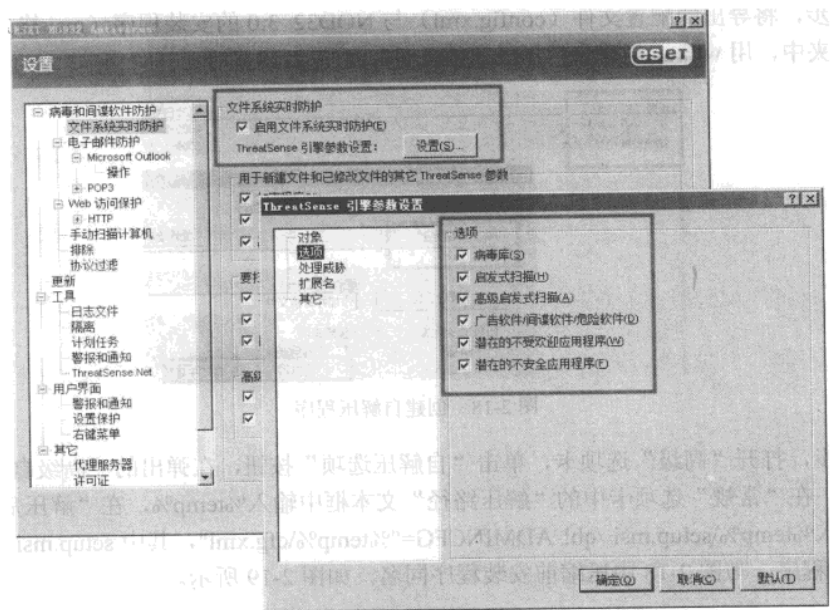


图 2-16 设置文件实时防护选项

第 2 步，设置每一个选项后，导出 NOD32 3.0 的配置。在 NOD32 的控制台界面中，在“设备”菜单中选择“导入/导出设置”命令，在弹出的“导入和导出设置”对话框中，选择“导出设置”单选按钮，在“文件名”文本框中设置导出配置文件的路径与配置文件名，例如 e:\config.xml，如图 2-17 所示。

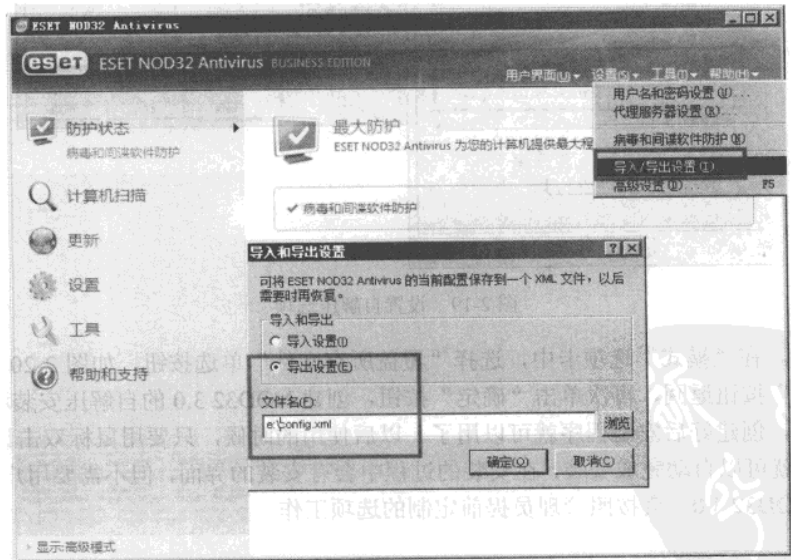


图 2-17 导出配置文件

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 3 步，将导出的配置文件（config.xml）与 NOD32 3.0 的安装程序（msi 格式）放在同一个文件夹中，用 winrar 创建自解压的压缩文件，如图 2-18 所示。

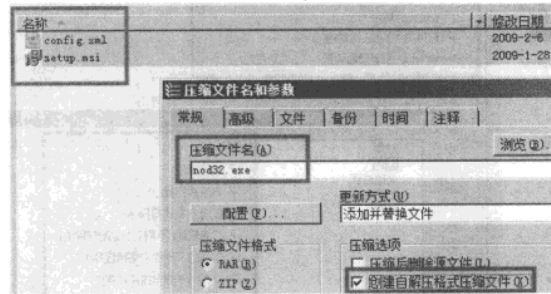


图 2-18 创建自解压程序

第 4 步，打开“高级”选项卡，单击“自解压选项”按钮，在弹出的“高级自解压选项”对话框中，在“常规”选项卡中的“解压路径”文本框中输入%temp%，在“解压后运行”文本框中输入%temp%\setup.msi /qb! ADMINCFG="%temp%\cfg.xml"，其中 setup.msi 是 NOD32 3.0 的安装程序，与图 2-18 中压缩前安装程序同名，如图 2-19 所示。

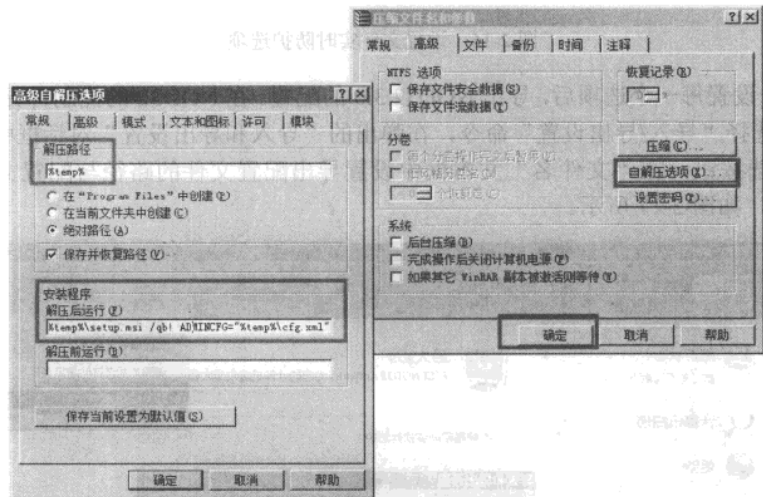


图 2-19 设置自解压选项

第 5 步，在“模式”选项卡中，选择“覆盖所有文件”单选按钮，如图 2-20 所示。然后单击“确定”按钮返回，再次单击“确定”按钮，创建 NOD32 3.0 的自解压安装程序。

第 6 步，创建好后安装程序就可以用了。以后使用的时候，只要用鼠标双击该安装程序，NOD32 3.0 就可以自动完成安装，在安装的过程中会有安装的界面，但不需要用户交互。安装完成后的 NOD32 3.0，会按照管理员提前定制的选项工作。

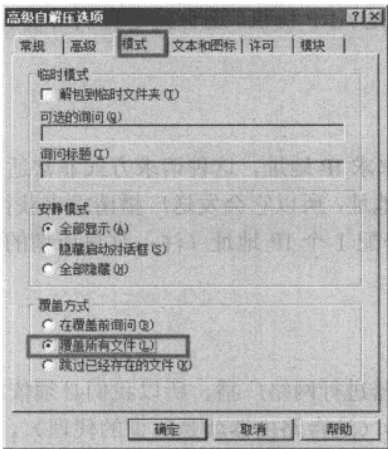


图 2-20 覆盖所有文件

2.3 防治 ARP 病毒的经验

ARP 病毒是现在比较流行的局域网病毒，也是破坏性比较大的一种病毒。预防 ARP 病毒就成了维护局域网安全的中中之重。要预防 ARP 病毒，首先要了解它的工作原理和工作方式才能更好的进行预防。

本节将介绍关于 ARP 病毒的一些基本知识和防治 ARP 病毒的一些经验，希望对读者有所帮助。

2.3.1 关于 ARP 的一些知识小总结

ARP 病毒一直以来是局域网的一大杀手。我们几乎每一个人也都听说过 ARP 病毒，但又有多少人知道 ARP 是什么？别说一般用户就是网管员相信也有不知道的。俗话说想要打败对手首先要了解对方，所以本节将介绍一下 ARP 的一些相关知识。如果在局域网中没有了 ARP，即使我们知道了一个工作站的计算机名，知道了一个工作站的 IP 地址，我们还是找不到它，就像我们知道一个地方叫“潘宁的家”，但是，不知道这个地方所处城区，街道，门牌号。那么，我们一样的找不到准确的位置，所以就不会实现局域网的互联。那么，ARP 在我们的局域网中有几种工作形式呢？接下来将介绍一下 ARP 的 4 种工作形式。

1. 正向 ARP

地址解析协议(Address Resolution Protocol)ARP，通过遵循该协议，只要知道了某台计算机的 IP 地址，即可以知道其物理地址。在 TCP/IP 网络环境下，每个主机都分配了一个 32 位的 IP 地址，这种 Internet 地址是在网际的范围上标识主机的一种逻辑地址。为了让报文在物理网路上传送，必须知道对方目的主机的物理地址。这样就存在把 IP 地址变换成物理地址的地址转换问题。以以太网环境为例，为了正确地向目的主机传送报文，必须把目的主机的 32 位 IP 地址转换成为 48 位以太网的地址。这就需要在互连层有一组服务将 IP 地址转换

网管天下 网管经验谈

为相应物理地址，这组协议就是 ARP 协议。这也就是我们常说的正向 ARP，另外三种是 ARP 的变形。

2. 反向 ARP

反向 ARP 是知道 MAC 来求 IP 地址，这种请求方式非常适用于无盘工作站，因为它无法从自身的操作系统中获得 IP 地址，所以它会发送广播请求来获得 IP 地址信息，而 RARP 服务器则会响应该请求消息为其分配 1 个 IP 地址（注：这里所谓的 RARP 服务器指的是 BOOTP 或 DHCP 服务器）。

3. 代理 ARP

因为 ARP 无法通过路由器进行网络广播，所以我们必须依靠一个设备来进行跨网段数据的传送，这个设备就是路由器（这台路由器就是所谓的代理）。我们要以一台路由器为代理，让发送方的 ARP 请求来确定该路由器的硬件地址，并将数据包发送到默认网关，最后由路由器按照自己的方式来转发数据。但是如果以这种形式来进行 ARP 的请求会出现这样一种状况，因为 ARP 请求是无法跨网段的，所以只能发送到路由器让路由器去转发，而发送方的 ARP 缓存表中存放的应该是路由器的硬件地址。在 IOS 中，默认情况下代理 ARP 功能是打开的，可以在每个接口上使用命令 `no ip proxy-arp` 关闭此功能。

4. 无故 ARP

主机偶尔也会使用自己的 IP 地址作为目标地址发送 ARP 请求。这种 ARP 请求称为无故 ARP，通常用于以下情况。

（1）无故 ARP 可以用于检测网络中的重复 IP 地址。一台设备可以向自己的 IP 地址发送 ARP 请求，如果收到 ARP 响应则表明网络中存在重复地址。

（2）无故 ARP 还可以通告一个新的 MAC。当一台设备收到一个 ARP 请求，如果 ARP 高速缓存中已有发送者的 IP 地址，那么此 IP 地址所对应的硬件地址将会被发送者新的硬件地址所更新，这种无故 ARP 用途正是基于此。

（3）某个子网中运行 HSRP 协议的路由器如果从其他路由器变成了主路由器，它将会发送一个无故 ARP 更新该子网内主机的 ARP 缓存。

说明 在 IOS 中默认是关闭的，但可以通过命令 `ip gratuitous-arps` 激活。世间万物，都有两面性，ARP 也不例外。它在为我们提供方便的同时，也一样将它的弊端丢给了我们这些受益者。

ARP 协议的缺陷：ARP 协议是建立在信任局域网内所有结点的基础上的，它很高效，但却不安全。它是无状态的协议，不会检查自己是否发过请求包，也不管（其实也不知道）是否是合法的应答，只要收到目标 MAC 是自己的 ARP reply 包或 ARP 广播包（包括 ARP request 和 ARP reply），都会接受并缓存，缓存时间一般为 20 分钟。

高速缓存技术（caching）：在每台使用 ARP 的主机中，都保留了一个专用的高速缓存区（cache），用于保存已知的 ARP 表项。一旦收到 ARP 应答，主机就将获得的 IP 位址与物理位址的映像关系存入高速 cache 的 ARP 表中。当发送信息时，主机首先到高速 cache 的 ARP

表中查找相应的映像关系。若找不到，再利用 ARP 进行地址解析。利用高速缓存技术，主机不必为每个发送的 IP 资料包使用 ARP 协议，这样就可以减少网络流量，提高处理的效率。

为了保证主机中 ARP 表的正确性，ARP 表必须经常更新。如何维护 ARP 表的有效性？ARP 表中的每一个表项都被分配了一个定时器，一旦某个表项超过了计时时限，主机就会自动将它删除，以保证 ARP 表的有效性。由于多数网络通信都需要持续发送多个信息包，所以即使高速缓存去保存一个小的 ARP 表也可以大大提高 ARP 的效率。就是因为这样的原因，就为 ARP 欺骗提供了可能，恶意结点可以发布虚假的 ARP 报文从而影响网内结点的通信，诸如网上现在经常提到的假冒网关，中间人攻击之类的异常情况就出现了。

2.3.2 关于防治 ARP 的一些经验

俗话说要想击败对手，首先要了解对手。本节内容就是了解 ARP 病毒和防治 ARP 的一些小经验。首先了解 ARP 变种病毒的特性：

- (1) 破坏你的 ARP 双向绑定批处理。
- (2) 中毒计算机改变成代理服务器又叫代理路由。
- (3) 改变路由的网关 MAC 地址和 Internet 网关的 MAC 地址一样。

新的 ARP 病毒发作情况：现在的 ARP 变种不是攻击客户机的 MAC 地址和路由由内网网关而是直接攻击你路由的 MAC 地址和外网网关；而且直接就把绑定 IP、MAC 的批处理文件禁用了。一会儿全掉线，一会儿是几台几台的掉线；而且中了 ARP 的计算机会将其转变成内网的代理服务器进行盗号和发动攻击。如果发现中了 ARP 没有掉线，那说明你中了最新的变种，你只要重启了那台中了 ARP 病毒的计算机，那么受到 ARP 攻击的计算机就会全部掉线，内网的网关不掉包，而外网的 IP 和 DNS 狂掉，该病毒发作时候的特征为，中毒的计算机会伪造某台计算机的 MAC 地址，如伪造其 MAC 地址为网关服务器的 MAC 地址。这样对整个局域网都会造成影响，用户表现为上网经常瞬断。

首先要做的就是先把中毒的机器找出来，方法就是在任意客户机上进入命令提示符（或 MS-DOS 方式），执行“arp -a”命令查看，这样就会看到有两个机器的 MAC 地址一样，而事实是所有的 MAC 地址都是全世界唯一的。然后再做一下实际检查就不难找到中毒机器了。

了解了 ARP 攻击的原理，接下来介绍全面的防治解决方法，采用下面的解决方法二结合方法三，效果就不错了，当然最好再加上交换机绑定 MAC 地址、服务器端绑定 IP、MAC。

1. 采用客户机及网关服务器上进行静态 ARP 绑定的办法来解决

- (1) 在所有的客户机上做网关服务器的 ARP 静态绑定。

首先在网关服务器（代理主机）的计算机上查看本机 MAC 地址：

```
C:\WINNT\system32>ipconfig /all
Ethernet adapter 本地连接 2:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel? PRO/100B PCI Adapter (TX)
Physical Address. . . . . : 00-1E-90-40-5D-81
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.0.1
Subnet Mask . . . . . : 255.255.255.0
```

网管天下 网管经验谈

然后在客户机的 DOS 命令下做 ARP 的静态绑定：

```
C:\WINNT\system32>arp -s 192.168.0.1 00-1E-90-40-5D-81
```

注
·
意

如有条件，建议在客户机上做所有其他客户机的 IP 和 MAC 地址绑定。

(2) 在网关服务器（代理主机）的计算机上做客户机的 ARP 静态绑定，首先在所有的客户机上查看 IP 和 MAC 地址，命令如上。然后在代理主机上做所有客户端服务器的 ARP 静态绑定。如：

```
C:\winnt\system32> arp -s 192.168.0.23 00-1b-2f-1a-81-90
C:\winnt\system32> arp -s 192.168.0.24 00-21-3f-54-90-88
C:\winnt\system32> arp -s 192.168.0.25 00-1e-45-69-91-66
```

(3) 以上 ARP 的静态绑定最后做成一个 Windows 自启动文件，让计算机一启动就执行以上操作，保证配置不丢失。

(4) 有条件的用户可以在交换机内进行 IP 地址与 MAC 地址绑定。

注
·
意

IP 和 MAC 进行绑定后，更换网卡需要重新绑定，因此建议在客户机安装杀毒软件来解决此类问题。

2. 网管路由对客户机使用静态 MAC 绑定

(1) 在网管路由上对客户机使用静态 MAC 绑定。ROUTE OS 软路由的用户可以参照相关教程，或是在 IP--->ARP 列表中——选中对应项目单击右键选择“MAKE STATIC”命令，创建静态对应项。

用防火墙封堵常见病毒端口：134-139，445，500，6677，5800，5900，593，1025，1026，2745，3127，6129 和 P2P 下载。

(2) 在客户机上进行网关 IP 及其 MAC 静态绑定，并修改导入如下注册表。

① 禁止 ICMP 重定向报文。

ICMP 的重定向报文控制着 Windows 是否会改变路由表从而响应网络设备发送给它的 ICMP 重定向消息，这样虽然方便了用户，但是有时也会被他人利用来进行网络攻击，这对于一个计算机网络管理员来说是一件非常麻烦的事情。通过修改注册表可禁止响应 ICMP 的重定向报文，从而使网络更为安全。修改的方法是：打开注册表编辑器，找到或新建“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters”分支，在右侧窗口中将子键“EnableICMPRedirects”（REG_DWORD 型）的值修改为 0（0 为禁止 ICMP 的重定向报文）即可。

② 禁止响应 ICMP 路由通告报文。

“ICMP 路由公告”功能可以使他人的计算机的网络连接异常、数据被窃听、计算机被用

安全方面 | 2

于流量攻击等，因此建议关闭响应 ICMP 路由通告报文。修改的方法是：打开注册表编辑器，找到或新建“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters\Interfaces”分支，在右侧窗口中将子键“PerformRouterDiscovery” REG_DWORD 型的值修改为 0（0 为禁止响应 ICMP 路由通告报文，2 为允许响应 ICMP 路由通告报文）。修改完成后退出注册表编辑器，重新启动计算机即可。

③ 设置 arp 缓存老化时间设置。

默认情况下 ARP 缓存的超时时限是两分钟，你可以在注册表中进行修改。可以修改的键值有两个，都位于“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”。

键值 1：ArpCacheLife，类型为 Dword，单位为秒，默认值为 120。

键值 2：ArpCacheMinReferencedLife，类型为 Dword，单位为秒，默认值为 600。

注：
意

这些键值默认是不存在的，如果你想修改，必须自行创建；修改后重启计算机后生效。

3. 安全模式下删除 system32\npptools.dll

ARP 病毒缺少了 npptools.dll 这个文件根本不能运行，目前所发现的 ARP 病毒通通提示 npptools.dll 出错，无法运行。暂时还没发现可以自动生成 npptools.dll 的病毒，npptools.dll 本身就 40 多 KB，病毒如果还要生成自己的运行库，不是几十 KB 的大小就可以办到的，再大一些的就不是病毒了。当然，还是要做 ARP-S 绑定，只绑定本机自身跟路由即可，可以在“一定程度上”减少 ARP 程序的破坏。还有外网的网关也必须和 MAC 地址绑定才安全。

说：
明

要删除该文件需要先关闭文件保护，最简单的方法就是用 XPLITE 来关闭，还有这个方法只对 ARP 病毒生效，对恶意软件只是小部分有效的。

2.4 数据安全方面的经验

保证数据的安全是网络维护和管理的核心内容，要保证数据的安全首先要了解一下数据保护的基本常识，和对数据进行加密的方法。总之，保证数据的安全就是要保证数据不被破坏而且不会把有效的数据被别人窃取。

2.4.1 数据保护常识小总结

作为网管员，也时常会遇到这种情况：某员工急急忙忙来找自己声称有重要的文件丢了，问能不能想办法把它找回来。事实上，与其在事情发生后很头疼的去补救，何不在事情没发生之前就想办法防止呢。而做为网管员管理的服务器，更需要重视数据的保护。所以本节就介绍一下防止数据丢失，需要注意的 10 条经验。

（1）硬盘读取数据时千万不要断电。

网管天下 网管经验谈

- (2) 电脑开机状态下不要搬动机箱。
- (3) 定期备份重要数据，并且备份数据后要确认备份的数据是否完整。
- (4) 计算机必须放置在满足以下条件的地方：温、湿度合适的地方；清洁的地方；没有人走动的地方；没有震动的地方。
- (5) 请慎重使用 FDISK, NDD 等磁盘操作软件。
- (6) 要经常使用杀毒软件，并且确保定期升级。
- (7) 当丢失数据时，千万不要随意使用数据恢复等软件，以免恶化损伤程度。
- (8) 建议使用 UPS 等确保供电的设备，防止计算机突然断电引起对硬盘的损伤。
- (9) 硬盘出现嘎嘎响声时尽量不要开机，要立即向专业人士请教。
- (10) 一般情况下不要打开机箱外壳，除非计算机故障或升级硬件。

2.4.2 加密保证数据安全的总结

“加密”这个词会令人联想到间谍、秘密活动和第二次世界大战的密码破解者解密敌人的信息。实际上，任何企业都能够方便地使用这种工具保守敏感信息的机密和安全，防止偷窥的眼睛。遗憾的是，许多企业没有利用加密技术的优势。它们担心加密技术太复杂，很难在日常工作中使用。实际上，加密重要的数据并不比运行病毒扫描软件和数据备份程序更困难。所以作为网管员对“加密”是要有所了解的，也许哪天单位会有这方面的需求。那么要让企业用上“加密”技术，作为网管员需要了解以下 4 点。

(1) “加密”的基础知识。

有两种加密数据的基本方法，一种方法是使用不对称 PKI（公共密钥基础设施）加密。PKI 密码技术是以一对密码密钥为基础的：一个是私人密钥，只有用户自己知道；另一个是公共密钥，是通信的对方知道的。

PKI 技术提供私人性和保密性、访问控制、文件传输证明和文件存档与提取报告。虽然多数安全厂商目前在其软件中都采用了某种类型的 PKI 技术，但是设计和实施中的差异阻碍了产品之间的兼容性。

加密数据的另一种方法是对称密钥保护，也做“密钥”加密。一般来说，对称加密方法加密和解密信息都使用相同的密钥，因此速度较快，但是没有 PKI 安全。当密钥的分配仅限于可信赖的少数人的时候，对称技术的工作是最好的。由于对称加密很容易破解，这种技术主要用于保护相对不重要的信息或者仅需要短时间保护的文件。

(2) 应用“加密”的介绍。

使用加密最简单的方法是购买一种商业应用程序或者一种采用某种加密技术的硬件产品。例如，微软的 Outlook Express 电子邮件客户端软件提供了内置的加密支持。同时，有些厂商已经开始在硬盘中采用加密技术。

由于大多数软件应用程序和硬件产品都不包括任何类型的内部加密技术，企业主和经理需要寻找单独的加密产品。这是一个令人困惑的过程。一个最好的方法是首先准确地确定企业的安全要求，然后找到能够满足每一个需求的加密产品。

微软 Vista 企业版和终极版用户可以使用 BitLocker 硬盘加密工具。这个整个硬盘的加密工具可提供强大的 1024 位加密。另一种 Windows 产品是 EFS（加密文件系统），这个工具使用对称 PKI 技术提供文件加密。

除了微软之外，主要加密厂商和产品包括 PGP、开源软件的 TrueCrypt、DEStlock+、Namo FileLock 和 T3 基本安全。

(3) 了解“加密”内容。

- 硬盘：一个企业可以选择加密整个硬盘作为减少或者消除数据被盗的方法。
- 个人文件：在整个硬盘加密有些小题大做的地方，逐个文件进行加密将根据需要提供增加的安全措施。许多主要加密产品提供用鼠标拖放加密功能。
- 笔记本电脑：与办公系统不同，笔记本电脑很容易丢失，很容易被偷窃。通过确保笔记本电脑上的内容不可读，企业能够把损失限制在仅是一台笔记本电脑的成本。越来越多的政府管理部门和保险公司都要求企业加密离开其环境的任何数据。
- 可移动存储设备：存储棒、拇指硬盘和类似的便携式存储技术提供了便携性和方便，同时也提供了数据丢失和被窃的机会。同笔记本电脑一样，加密将把企业的损失仅限制在设备成本本身。越来越多的可移动存储设备配置了内置的加密支持。
- 文件传输设备：在没有加密的线路或者无线链路上发送文件能够把敏感的信息暴露给数据窃贼。加密能够提供一层额外的安全保护，即使是在使用一个安全的网络的时候也是如此。
- 电子邮件：加密的电子邮件在传输过程中和在收件人的信箱中能够保持秘密状态。
- 即时消息：越来越多的企业使用即时消息交换保密的商业信息，加密有助于保证这些重要信息传输的安全。

(4) “加密”的局限性。

同任何技术一样，加密软件并不是十全十美的。即使是最好的产品也要消耗处理器的速度和存储的空间。用户还会丢失或者忘记口令，从而使系统永远锁死。

在购买任何加密工具之前，用户要认真研究这个产品。确保这个产品能够解决你的公司的需求，兼容你现有的系统，在可靠性和技术支持方面有良好的跟踪记录。

2.5 数据恢复方面的经验

本节主要介绍了作为网络管理员如何保存数据和当数据遭到破坏和误删除时应该怎样做有效的恢复，以及如何对数据进行备份，以便及时恢复丢失的数据，将损失减到最小。

2.5.1 保存数据的注意事项与数据恢复方法总结

对于做网管员的人来说，保证企业数据的完整和安全未尝不是最艰巨的任务之一。因为不确定因素太多了，中毒、断电、保存不当和系统故障，甚至硬件故障这些都有可能成为企业重要数据的杀手。所以保障数据的安全和完整是网管员的必修课，本节内容就是介绍一些保存数据的注意事项，以及恢复数据的经验。

1. 怎样保护重要的数据

从本质上来说，大多数的数据丢失，都是由于使用者的不良习惯或使用不当引起的。所以在保存数据时，应做到以下几点。

- (1) 合理规划硬盘，合理划分分区，并且为每个分区设置英文的卷标。如果有多个硬盘，

网管天下 网管经验谈

从卷标上可以分辨出所在硬盘及分区。

(2) 对于热衷安装多系统的用户，优先使用 PQ-Magic 的 BootMagic，其次是操作系统自带的引导程序，不推荐使用 BootStar、SFdisk。在计算机硬件配置比较高的时候，优先使用 VMware Workstation 或 Virtual PC 的虚拟机来安装、测试多系统。

(3) 不把数据保存在系统分区（通常来说，就是 C 盘），这包括：不把数据保存在“桌面”上；修改“我的文档”的默认路径；不把数据保存在系统分区的一个或多个文件夹中，而是把数据保存在其他分区。

(4) 对于某些品牌机来说，默认的系统分区很大，可以使用 PQ-Magic 重新调整分区大小或者重新分区。

(5) 重要数据要及时备份，并且及时用最新的备份设备对以前备份的数据进行备份。

(6) 不把 U 盘、活动硬盘当成“永久”备份设备。在向 U 盘、活动硬盘上存储数据时，在本地计算机或者其他设备上再做一次备份。因为 U 盘、活动硬盘本身就是“不可靠”的数据。

(7) 不要把重要数据保存在 Internet 上的邮箱或网络存储中，即使你使用的是一个商业供应商提供的服务。一定要记住，只有数据保存在自己的手里，才是安全的。

(8) 在保存有重要数据的计算机或服务服务器上，不要浏览不可靠的网站，也不要测试或者运行一些不可靠的软件。这些计算机如果安装的是 Microsoft 的产品，请及时的打补丁。

2. 数据恢复的基本操作步骤

当某个员工或某领导遇到数据丢失时，网管员应该按照下面的流程进行处理。

(1) 详细询问硬盘数据丢失的原因。首先要询问数据丢失的原因，是误删除、误格式化、误分区等误操作行为，还是硬盘突然丢失或无法读写，并且还要询问故障发生后，用户自己还做过哪些操作。

(2) 误操作的数据恢复。对于误操作造成的数据丢失，如果是误删除、误格式化，可以在你自己的计算机上安装数据恢复软件如 EasyRecovery 6.1，并将需要恢复数据的硬盘接到一个没有问题的主机上做并设置为从盘（通过设置跳线），从而进行数据恢复的操作。这个过程一般需要很长时间。

如果是误分区造成的数据丢失，使用 diskman，在一台计算机上接上用户硬盘，拆下计算机上原来的硬盘，使用光盘或软盘启动计算机，使用 DiksMan 恢复分区。在恢复分区的时候，要询问用户，硬盘原来有几个分区、分区的类型是 FAT32 还是 NTFS、每个分区的大致大小。如果用户不清楚硬盘分区的数量、大小、分区类型，要根据经验进行判断。例如，如果用户是在 2000 年~2004 年左右的计算机，那硬盘可能是 20 GB~80 GB 左右，通常是 FAT32 分区；如果用户使用的是 NTFS 分区，说明用户有一定的“水平”，他应该知道分区的类型。这时的硬盘通常是 3~5 个左右分区。如果是在 2004 年之后的计算机，硬盘可能是 120 GB~250 GB 甚至更大，则用户的分区可能是 NTFS，也可能是有 4 个以上的 FAT32 分区。在使用 DiskMan 恢复的时候，在纸上记下每次恢复的大小等情况，恢复之后，在 DOS 下尝试列目录，当显示出目录信息时，表示恢复正确。

(3) 突发问题引起的数据丢失。如果是由于各种意外原因造成的数据或者分区丢失，这时应首先检查硬盘的电路板有无明显的烧灼痕迹，避免因该硬盘的电路损坏再次造成计算机主机的损坏。如硬盘无明显的电路损坏，把硬盘加电试机，看在 CMOS 中是否能够找到硬盘。

如果可以检查到硬盘，表示启动系统后（用其他好硬盘启动系统，将等待修复的硬盘设

安全方面 | 2

成从盘），如果硬盘分区信息可见，并且分区内容可读，则使用“数据恢复软件”恢复；如果恢复出的数据有错误，可以使用“数据修复软件”修复文档。通常情况下，我们使用专用设备能做到的就是：分区恢复、数据恢复、数据修复、密码修复等。将数据转移到安全区域，找到数据后，将找回的数据复制到另一块物理硬盘上，一定不能复制在同一块硬盘的不同分区。如果条件许可，可以将恢复的数据用刻录机刻成光盘，交给用户，任务完成。

如果自检找不到硬盘，硬盘自检不到的情况多数都是硬件方面的问题，又可分为主板的硬盘控制器（包括 IDE 接口断针，短针，接触不良，虚焊等）故障和硬盘本身的故障。如果问题在主板上，那么数据不会受到破坏，把硬盘接在别的计算机上就可以正常读出。如果问题出在硬盘上，并不是所有的故障都能修复。硬盘的故障又可细分为控制电路，主轴电机，磁臂电机和磁头，磁头放大器和盘片，数据接口等。如果是控制电路的问题，可以在更换控制芯片后，把数据正常读出。如果是电机、磁头和盘片的故障，一般计算机市场是没有修理能力的，需要返回原厂或者找专业数据恢复机构进行恢复。

3. 数据恢复软件

关于下面这些软件的使用，在这里不再进行介绍，大家可以在“百度”等搜索引擎找到相关的软件和使用方法。

- (1) 分区恢复软件 diskman (diskgen)。
- (2) 最简单的数据恢复软件 Recover4All。
- (3) EasyRecovery 6.1。
- (4) 专业数据恢复软件 Final Data。
- (5) 可以通过网络进行数据恢复的软件 R-Studio 4.0。

4. 数据修复软件

- (1) Office 类文档修复软件。
- (2) MP3 文件修复软件。
- (3) 影音、视频文件修复软件。
- (4) RAR、ZIP 文件修复软件。
- (5) PDF 文件修复软件。
- (6) SQL Server 数据库修复软件。

5. 密码恢复软件

- (1) Office 类密码恢复软件。
- (2) 去除 PDF 密码保护软件。
- (3) 破解 RAR、ZIP 密码软件。
- (4) 破解开机密码、Windows XP/2003 管理员密码软件。
- (5) 解密 EFS 加密的文件。

2.5.2 误删除误分区的恢复经验

用 Fdisk 命令删除了硬盘分区之后，表面现象是硬盘中的数据已经完全消失，在未格式化

网管天下 网管经验谈

时进入硬盘会显示无效驱动器。如果你了解 Fdisk 的工作原理，就会知道 Fdisk 只是重新改写了硬盘的主引导扇区（0 面 0 道 1 扇区）中的内容，具体地说就是删除了硬盘的分区表信息，而硬盘中任何分区的数据均没改动。可仿照“分区表错误”的修复方法，即想办法恢复分区及数据，但这只限于删除分区或重建分区之后；如果已经对分区用 Format 命令格式化，需在恢复分区之后，再恢复分区数据。针对以上介绍的几种误删除类的数据恢复，为了提高恢复成功率，必须遵循如下几点。

1. 文件或文件夹的恢复

不向目标分区写入新文件，从概念上容易理解，但实际要做到却不是那么容易的。因为 Windows 会在各个分区多多少少生成一些临时文件，加上还有在启动时自动扫描分区的功能，如果设置不当或操作上稍不留意，可能已经写入了新文件而你还不知道。

（1）不要安装新软件或运行新任务。特别是不要向恢复目标分区安装新的软件，即使是恢复软件本身。例如你要恢复的是 C 盘被误删除的数据，而工具软件的默认指向都是 C 盘的，你一路 Enter 安装的话，可能就万事休矣；如果你的虚拟内存设在了 C 盘，此时也不要打开新的任务，以免因为虚拟内存的更新变化覆盖数据。你应该在“系统”里更改虚拟内存的指向路径，然后重新启动 Windows，再安装恢复软件到目标以外的分区。

（2）注意 Windows 扫描和报告的设置。默认状态下，Windows 会在启动的时候检测分区有没有错误，如果上次是非正常关机，你就会看到一个扫描的任务及进度条，这种扫描对解决交叉链接错误有用，但对于要恢复的文件可能会造成致命的破坏——因为扫描完毕后，Windows 会生成信息报告，有可能刚刚（占用）破坏目标文件的关键字节，如果是可执行文件，就算勉强恢复过来也用不了。进入 Windows 后，也请你不要在该目标分区进行磁盘扫描，因为默认状态下，Windows 会把交叉链接文件和文件碎片转化成*.CHK，也有可能破坏你的目标文件。如果你用的是 Windows98，建议你在 MSDOS.SYS 里设置一下，在 Option 组加入一句 AutoScan=0，把启动的扫描屏蔽掉；如果是 Windows2000 或 XP，就按 Enter 键跳过磁盘检测直接进入 Windows。

（3）操作恢复的技巧。恢复工具的扫描技巧一般来说，误删除文件都是马上发现自己的误操作，所以刚删除的文件在磁盘里的文件分配表处于较靠前的位置，我们可以利用这一点，加快恢复的速度。例如你运行了 EasyRecover，在选定了目标分区后，只要扫描 5 左右的目录树，大概在 3000 个到 5000 个文件左右，就可终止扫描，然后进入下一步，一般都能找到。这种方式比完全扫描后再找恢复文件要容易，如果你扫描所有的文件，可能会有数万个甚至 10 多万个已经删除的列表，此时你要找自己想恢复的目标就比较困难了——因为在你的计算机里，不同时期可能产生过同一个文件名的几个文件，为了防止混乱，恢复软件一般会把这些类似的文件标记为开头，数字编号结尾的文件，你无法按首字母来找，要靠眼睛一个个识别，太多的选择会让你眼花缭乱。可以在终止扫描时，选择保存当前扫描进度，如果 5 的数量没找到你的目标，可以按此进度继续扫描，不必从头开始一次。注意这个保存操作也不要放到目标分区里，要另外指定路径存盘。DOS 时代的 UNDELETE 软件，只能处理 FAT 的格式，而且对于长文件名结构无能为力。

字处理软件相关文件的技巧，像 WPS 或 WORD 这类字处理软件，除了用恢复工具，还可以进入其安装目录，找到隐藏的临时文件直接恢复。因为这类软件都会对你当前操作的文件生成一个后备文件，而且不自动删除，所以你可以在 DOS 状态下，在目标目录输入

ATTRIB*.h 消除临时文件的隐藏状态，然后把后缀名改为*.DOC*或是.WPS，就可能已经成功恢复了。当然，得到的临时文件可能会很多，名字未必和原来的对应，所以只能一个个打开看看是哪一个。

2. 恢复分区的注意事项

此处说的主要是没有正确备份分区表的情况下，对分区的恢复；已经有分区表备份的恢复很简单，这里不再重复。

(1) NTFS 的格式不要急于重装系统：如果你使用的是 NTFS 格式，但 Windows 运行出了问题，即使分区表没有损坏，还能看到该分区，也不要急急忙忙地重装系统。因为 NTFS 是有限加密的，而且在一个操作系统下面加密的密钥是唯一的，如果你重装了系统，即使是同一个 2000 或 XP 版本，也有可能读不出 NTFS 加密的文件夹。低级格式化更是不要轻易尝试。

(2) 在用 NDD 等工具重建分区表之前，先备份现在的分区表状态：在用 KV 或 Norton 这类具有检测和重建分区表功能的软件操作前，请先把当前的分区表备份下来，即使目前是不正常的状态。这样是为了防止操作失败，导致更多的损失。在正常状态下，小心不要在杀毒软件里随便点“恢复分区表”，像 KV 系列，没事乱“恢复”的话有时会导致系统崩溃。

(3) 如果是误格式化了分区，最好先用 Ghost 备份镜像全盘到另外一个硬盘，再尝试各种工具进行恢复操作。一般来说，完全无损恢复是不太可能的了，只能恢复像 MP3，文档，邮件等独立的文件，对于一些要 VXD 设备文件，DLL 动态链接对话框运行的软件，完好地数据恢复不太可能。所以，对分区的操作一定要小心谨慎！

2.5.3 创建紧急修复磁盘

首次对服务器软件和硬件进行全面升级，需要为服务器创建一个紧急修复盘，以备日后服务器系统出现故障能及时修复。

在服务器首次投入使用和对系统做了某些重大更改（例如软件和硬件升级）时，应该使用备份创建紧急修复磁盘（ERD）。仅在使用其他方法（例如启动选项“安全模式”和“最后一次正确的配置”）无法进行系统恢复的情况下，才使用 ERD 做最后的尝试。

注
意

要执行此过程，必须是本地计算机上的管理员组或备份操作员组成员，或者已被授予适当的权限。如果计算机已加入域，则域管理员组成员也可以执行此过程。完成此步骤所需的工具是 Backup。还需要一张 1.44 MB 的空白软盘来创建紧急修复磁盘（ERD）。

要创建紧急修复磁盘（ERD），请执行以下步骤：

第 1 步，选择“开始”→“运行”命令，在“打开”文本框中输入“ntbackup”命令，然后单击“确定”按钮；或者选择“开始”→“程序”→“附件”→“系统工具”→“备份命令”，都可弹出如图 2-21 所示的“备份”窗口。

第 2 步，单击“紧急修复磁盘”按钮，当弹出“紧急修复盘”界面时，根据指示信息在驱动器 A 中插入 1.44 兆字节（MB）的软盘，如图 2-22 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

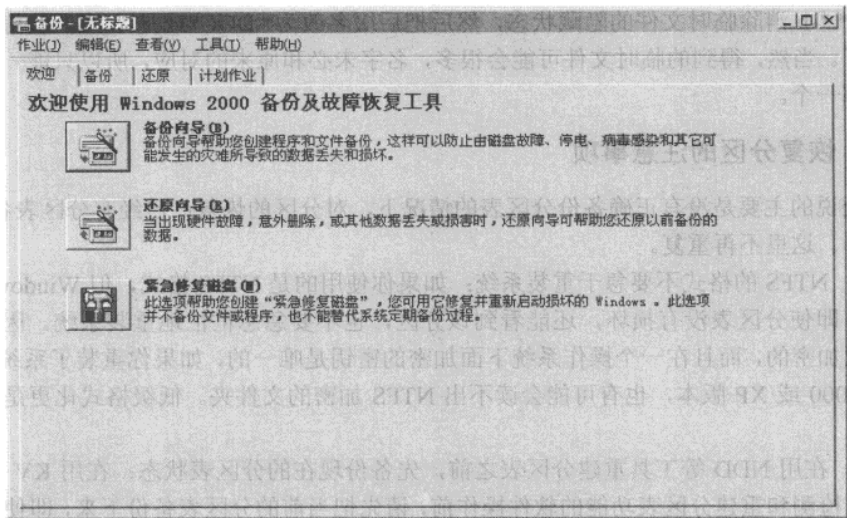


图 2-21 备份工具

第 3 步，选择“也将注册表备份到修复目录中。如果注册表损坏了，这种备份可用来帮助恢复你的系统”复选框，如图 2-22 所示。单击“确定”按钮时，会将当前的注册表文件保存到 systemroot\repair 文件夹内的一个文件夹中。这在硬盘发生故障，需要恢复系统时很有用。

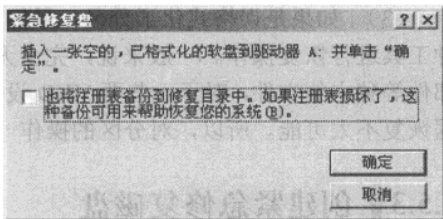


图 2-22 选择备份注册表

第 4 步，当紧急修复盘屏幕提示可以取出软盘时，对这个软盘进行标识，以便于将来识别。然后将软盘保存在计算机附近的安全位置，将来可以将此软盘与安装 CD 结合使用以启动和恢复计算机。

注 如果选择了“也将注册表备份到修复目录中。如果注册表损坏了，这种备份可用来帮助恢复你的系统”复选框，则在修复过程需要使用保存在 systemroot\repair 文件夹中的信息，切勿更改或删除此文件夹。

2.5.4 容灾所涉及的恢复技术

容灾（Disaster Recovery）项目的实施中涉及到多种技术。这些技术可以分为三类：应用恢复，网络恢复，数据恢复。

(1) 应用恢复技术。

常用的应用恢复技术或方法如下：

通过负载均衡提供永不停顿的系统运行能力（Tier-7）。

例如：IBMS/390 的 GDPS 技术给用户提供一个无中断的操作环境，来运行那些关键业务

的应用程序，通过自动应用恢复能力来满足其第 7 级容灾要求。

通过事先写好的脚本来实现自动的热接管（Tier-6）。

例如：GDPS 也可以在热待命状态下运行，来为 S/390 系统提供第 6 级解决方案。

HAGEO 提供与 GDPS 热待命相似的解决方案，并常被用来作为大型关键业务 UNIX 数据中心的 DR 解决方案。

按预案手工实现站点接管（Tier4/5）。

例如：有些设施的 DR 包括必须有人介入和决策的手动应用恢复程序。

在实际灾难发生时，一些这样的设施因为对人工操作的依赖，造成恢复过程的延误。因此，容灾的实施必须包括一定程度的自动化，这也是 GDPS 和 HAGEO 这样的软件的主旨。

(2) 网络恢复技术。

常用的网络恢复技术或方法如下：

4-7 层交换机（Tier-7）。

例如：无中断的第 7 级网络恢复需要动态网络路由重选，来保证应用能够在不中断最终用户的情况下转入备用数据中心。在 SNA 环境下通过 APPN 来完成，而在 IP 环境下则通过第 4-7 层转换来完成。APPN 是在 IBM S/390 GDPS 环境下，为动态网络恢复而开发的 SNA 网络技术。通过标准的基于路由器的技术，可以在通用的 IP 传输上使用 APPN。

路由（Tier-6）。

例如：在第 6 级 DR 的实施中，网络恢复可以通过 APPN 和/或标准的路由协议来完成（OSPF/EIGRP/BGP-4）在非 GDPS 环境中，APPN 应用路由在容灾系统备用路径可用时，自动恢复网络连接。

2 层 Reconnect（Tier-4/5）。

例如：SNA 子网在以太网/SNA 中通过 ATM/帧中继/DDN 链路进行互联，如果发生链路故障，则可以通过手工切换来实现网络恢复。

(3) 数据恢复技术。

数据容灾系统的实现可以采用不同的技术。一种技术是采用硬件进行远程数据复制，称为硬件复制技术。这种技术的提供者是一些存储设备厂商，其技术如 PPRC、SRDF。数据的复制完全通过专用线路实现物理存储设备之间的交换；另一种技术是采用软件系统实现远程的实时数据复制，并且实现远程的全程高可用体系（远程监控和切换）。这种技术的代表则是一些存储软件厂商，其技术如 HAGEO、VVR。

数据复制是一个复杂的议题，但一般来说，它可以在硬件或软件层上实施，如图 2-23 所示。

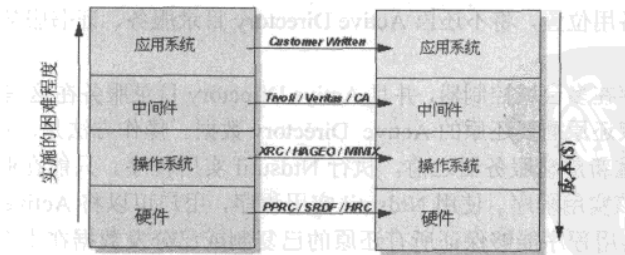


图 2-23 数据复制

如今，市场上的硬件和软件技术提供不同的第 4 级和第 7 级数据恢复，对硬件或软件的选择

网管天下 网管经验谈

择取决于很多与设施相关的因素，如工作量、网络成本要求、工作点和数据恢复点间的距离、同性或异性的平台支持等。

2.5.5 Windows Server 2003 的数据备份

利用 Windows Server 2003 系统的备份工具，创建一个服务器系统状态文件备份计划到磁带上。这一备份类型也就是通常所说的“系统状态备份”。

在 Windows Server 2003 系统中，系统状态文件所包括的组件，如表 2-1 所示。

表 2-1 可以备份的系统状态数据

组 件	该组件何时包括在系统状态中
注册表	总是
COM+ 类注册数据库	总是
启动文件，包括系统文件	总是
证书服务数据库	如果当前服务器为“证书服务”服务器
Active Directory 目录服务	如果这是一个域
SYSVOL 目录	仅当该服务器为域控制器
群集服务信息	如果处于群集中
IIS Metadirectory	如果已经安装
在 Windows 文件保护下的系统文件	总是

备份将这些系统组件作为系统状态数据，组成计算机系统状态数据的精确系统组件，将依赖于计算机的操作系统和配置。在 Windows XP Professional 系统中，系统状态数据只包含注册表、COM+ 类注册数据库、Windows 文件保护下的文件和启动文件等。而在 Windows Server 2003 家族操作系统中，系统状态数据包含注册表、COM+类注册数据库、Windows 文件保护下的文件和系统启动文件等。根据服务器的配置，系统状态数据中可以包含其他数据。例如，如果服务器是证书服务器，则系统状态还包含证书服务数据库；如果服务器是域控制器，Active Directory 和 SYSVOL 目录也包含在系统状态数据中；如果服务器是群集中的结点，则包括“群集”数据库信息；如果安装了 Internet 信息服务（IIS），则包括 IIS 配置数据库。

当选择备份或还原系统状态数据时，所有与计算机相关的系统状态数据将得以备份或还原。用户不能选择备份或还原系统状态数据的单独组件，这是由于系统状态组件间存在依存关系。然而，用户可以还原系统状态数据到备用位置。如果执行这个任务，只有注册表文件、SYSVOL 目录文件、群集数据库信息和系统引导文件被还原到备用位置。如果当还原系统状态数据时指派了备用位置，将不还原 Active Directory 目录服务、证书服务数据库和 COM+类注册数据库。

如果企业中存在多台域控制器，并且 Active Directory 目录服务在这些服务器中相互复制，那么用户必须授权还原需要还原的 Active Directory 数据。操作方法是，在还原系统状态数据之后，在网络中重新启动服务器之前，执行 Ntdsutil 实用程序。只能在服务器处于目录服务还原模式时运行该实用程序。使用 Ntdsutil 实用程序，用户可以将 Active Directory 对象标记为授权还原。该实用程序能够保证所有还原的已复制或已分发数据在本企业内正确地复制或分发。

例如，如果不经意地删除或修改了存储在 Active Directory 目录服务中的对象，并且这些对象已经复制或分布到其他服务器，那么必须授权还原那些对象以使它们复制或分布到其他服

安全方面 | 2

务器。如果不授权还原对象，那么它们决不会复制或分布到其他服务器，因为它们比其他服务器上的当前对象旧。使用 Ntfsutil 实用程序标记授权还原的对象可以确保要还原的数据在全组织内复制或分布。另一方面，如果系统盘发生故障或 Active Directory 数据库被损坏，那么用户可以在不使用 Ntfsutil 实用程序的情况下直接非授权还原数据。

Ntfsutil 命令行实用程序可以从命令提示符中运行。还可以通过在命令提示符处输入“ntfsutil /?”，来显示有关 Ntfsutil 实用程序的帮助。

注 · 意

系统状态数据包含系统配置的大多数元素，但可能不包含对系统进行故障恢复时所需要的全部信息。因此，建议在备份系统时备份全部启动和系统卷（包括“系统状态”）。虽然不能更改备份哪个系统状态组件，但是通过设置高级备份选项，可以备份所有带有系统状态数据的受保护的系统文件。具体将在后面进行详细介绍。

为了在域控制器上还原系统状态数据，必须首先以目录服务还原模式启动计算机。这将允许还原 SYSVOL 目录和 Active Directory。

只能备份和还原本地计算机上的系统状态数据，不能备份和还原远程计算机上的系统状态数据。

系统状态数据备份的具体步骤如下。

第 1 步，选择“开始”→“运行”命令，在“运行”文本框中输入 ntbackup 命令，然后单击“确定”按钮；或者选择“开始”→“程序”→“附件”→“系统工具”→“备份”命令，在 Windows Server 2003 系统中弹出如图 2-24 所示的“备份工具”窗口。

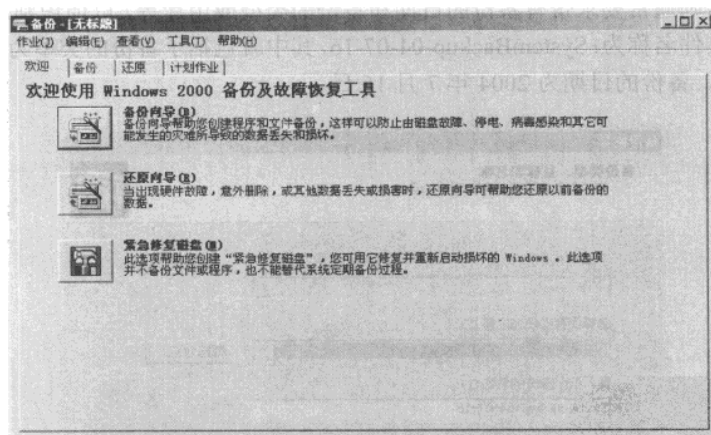


图 2-24 备份工具

第 2 步，单击“备份向导”按钮，弹出备份向导对话框。直接单击“下一步”按钮，弹出如图 2-25 所示的对话框。在这个对话框中要选择备份的数据内容，如果要备份整个计算机系统，则选择“备份这台计算机的所有项目”单选按钮；如果只是要备份某些指定的内容，则选择“备份选定的文件、驱动器或网络数据”单选按钮；如果只是要备份系统状态数据，则选择“只备份系统状态数据”单选按钮。本示例因为要进行系统备份，所以在此选择“只备份系统

状态数据”单选按钮。

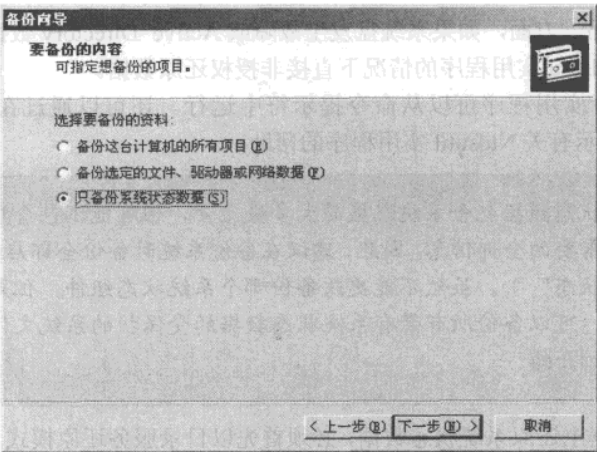


图 2-25 选择要备份的内容

第 3 步，单击“下一步”按钮，弹出如图 2-26 所示的对话框。在这个对话框中要求为所进行的备份活动指定一个名称和备份文件存放的路径。

备份文件存放位置既可以是本地磁盘（在企业备份中通常不这样选择），也可以是网络上其他计算机上的磁盘，还可以是磁带机、光盘机、磁带库或光盘库等之类的存储媒体。中小型企业通常选用磁带机，而大中型企业则通常选用磁带库、光盘塔和光盘库等大型的存储设备。至于备份文件名则通常要求带有备份的日期和备份的类型或用途等，以便识别。如作者此次进行的系统备份文件名称为：SystemBackup-04-07-16，其中就包括了备份的类型为“SystemBackup（系统备份）”，备份的日期为 2004 年 7 月 16 日。

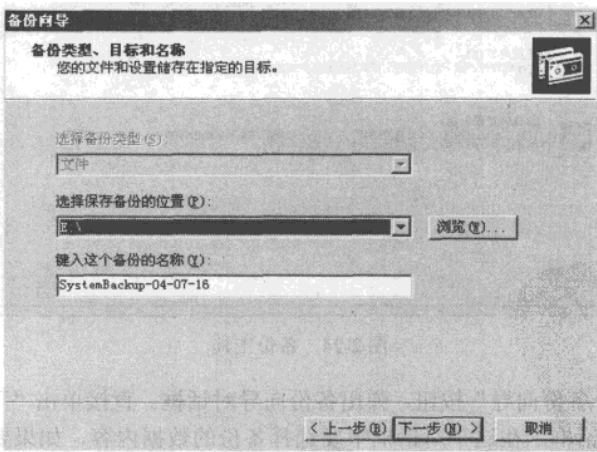


图 2-26 “备份类型、目标和名称”对话框

说
明

如果在如图 2-25 所示对话框中选择的是“备份选定的文件、驱动器或网络数据”单选按钮，则单击“下一步”按钮，弹出的是如图 2-27 所示的对话框。在这个对话框中要求选择要备份的文件夹（不能指定单个文件）。如果要备份某个磁盘或文件夹上的文件，则必须先单击相应盘符或文件夹前面的“+”号，展开各文件夹项，随后再一级级展开，直到出现要备份的文件夹。选好备份文件后单击“下一步”按钮，同样会弹出如图 2-26 所示的对话框。因为本示例备份的仅是系统状态数据，一般用户都无法知道全部的系统状态文件位置，所以备份文件的指定工作就由系统自动完成，没有出现如图 2-27 所示的对话框。

第 4 步，单击如图 2-26 所示的对话框中的“下一步”按钮，弹出如图 2-28 所示的“完成备份向导”对话框。其中显示了以上各步的设置摘要。单击“完成”按钮完成整个备份活动的设置。

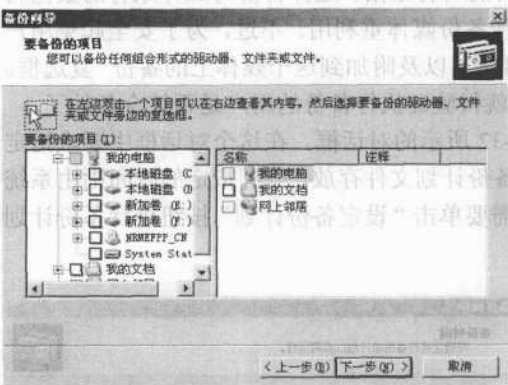


图 2-27 要备份的项目

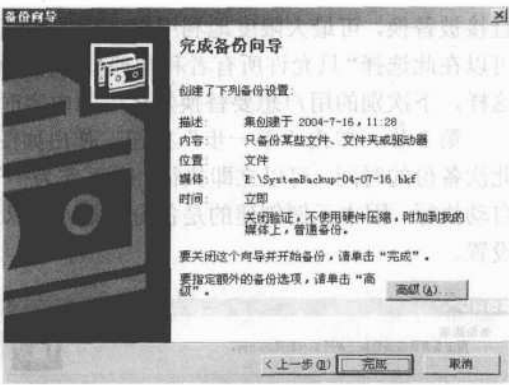


图 2-28 完成备份向导

第 5 步，因为以上没有对此次备份任务进行详细的设置，所以还需单击“高级”按钮进行一些高级备份选项的设置，弹出的对话框如图 2-29 所示。在这个对话框中可以选择此次备份活动所用的备份类型为“正常”。

第 6 步，单击“下一步”按钮，弹出如图 2-30 所示的对话框。在这个对话框中可以选择是否要启用备份后数据验证、硬件压缩功能（许多磁带机都具有此功能，启用后所支持的数据容量将扩大）和是否进行卷影复制。具体功能在各复选框下都有说明，不再赘述。在此可全不选。因此示例备份的仅是系统状态数据，所以卷影复制功能没有激活，且因当前所选用的磁盘设备不支持硬件压缩，所以该选项也没有被激活。又因为系统文件往往连续发生大量的更改，所以也无法对磁带上备份的系统状态数据进行验证，也就无需选择“备份后验证数据”复选框了（注意，如果要选择这一复选框，会很耗时间和服务器资源的，而且对磁带也有严重损耗）。

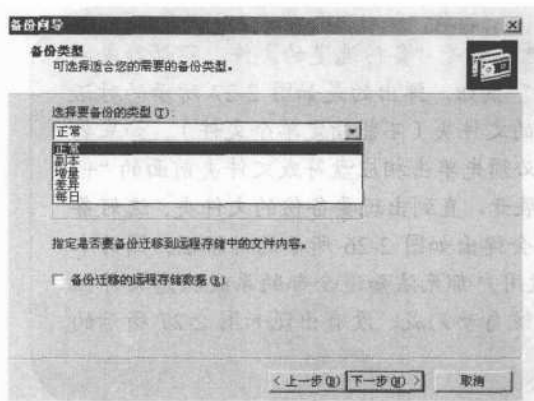


图 2-29 备份类型

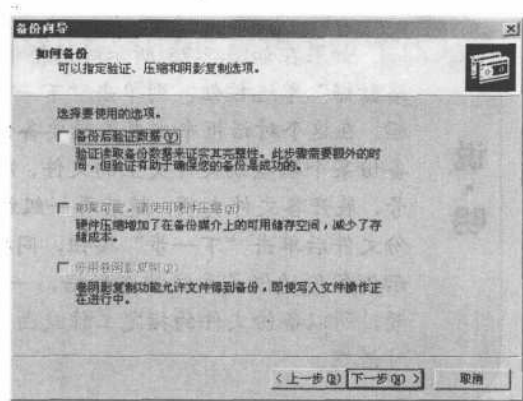


图 2-30 如何备份

第 7 步，单击“下一步”按钮，弹出如图 2-31 所示的对话框。在这个对话框中可以指定此次备份对媒体中现有备份的处理方式。通常是每次备份用一个全空的磁带进行，所以通常选择“替换现有备份”单选按钮，替换掉磁带中原有的所有数据。这样备份时媒体原有的数据将直接被替换，可最大限度地利用媒体空间，也可使备份媒体重用。不过，为了安全起见用户可以在此选择“只允许所有者和管理员访问备份数据，以及附加到这个媒体上的备份”复选框。这样，下次别的用户想要替换媒体中的内容时，就得验证执行备份的用户是否符合条件了。

第 8 步，单击“下一步”按钮，弹出如图 2-32 所示的对话框。在这个对话框中要求指定此次备份的时间。可以立即执行，也可作为一个备份计划文件存放，等到指定的时间则由系统自动执行。因本示例创建的是备份计划，所以还需要单击“设定备份计划”按钮进行备份计划设置。

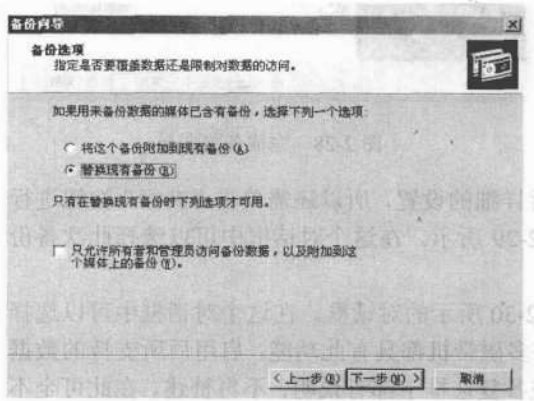


图 2-31 备份选项

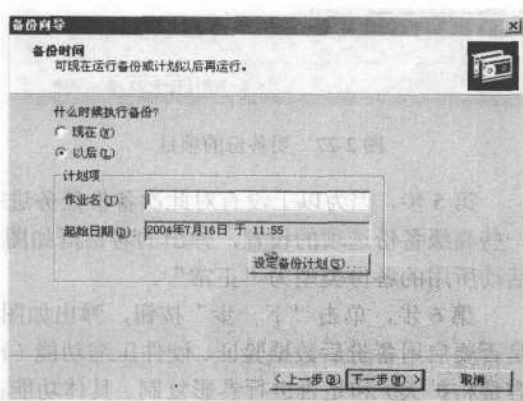


图 2-32 备份时间

第 9 步，单击“设定备份计划”按钮后弹出如图 2-33 所示的对话框。在其中可以具体设置备份计划开始的时间，还可通过单击后面的“高级”按钮，弹出如图 2-34 所示的对话框。在这个对话框中可以设置计划结束的日期和时间，其中有许多灵活的配置选项，可以进行设置。

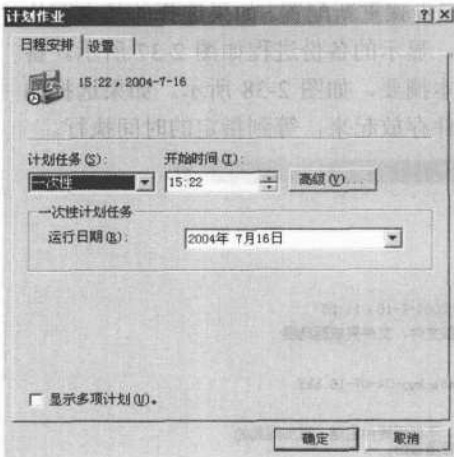


图 2-33 日程安排

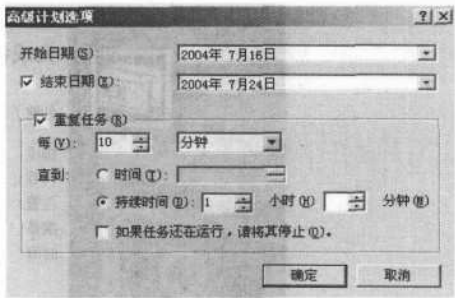


图 2-34 高级计划选项

除此之外，还可在如图 2-33 所示的对话框中设置计划的执行次数，本示例为一次性执行计划，所以需要在“计划任务”下拉列表框中选择“一次性”选项。其实其中还有许多其他选项，如每天、每周、每月、在系统启动时、在登录时和空闲时等，不同的选项所对应的配置界面不完全一样。也就是说这样一个备份计划可以在每天、每周或每月等多次重复进行，这对于配置类似的备份活动非常方便。除此之外，还可对备份计划进行一些备份选项详细设置，切换到如图 2-35 所示对话框中的“设置”选项卡。在这个对话框中可以对备份计划完成后所进行的步骤，以及空闲等时间和备份时的电源管理等选项一一设置，本示例不进行这方面的设置。

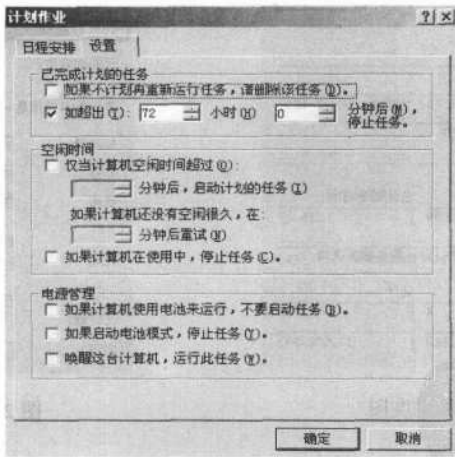


图 2-35 计划作业

以前在 Windows NT 4.0 系统上，要编写这样一个重复进行的备份计划非常麻烦，需要利用备份命令、脚本知识和批处理程序知识，编写一段小程序。现在则可以直接通过界面方式配置，非常直观，容易掌握。

第 10 步，以上配置好后单击“确定”按钮返回到如图 2-32 所示的对话框。单击“下一步”按钮，弹出如图 2-36 所示的对话框。这是一个向导完成对话框，在对话框中显示

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

了以上步骤设置的结果，如果认为有误可返回到相应步骤重新配置。如果选择的是立即执行方式，则单击“完成”按钮后系统立即进行备份，显示的备份进程如图 2-37 所示。备份完成后，在备份进度对话框中显示此次备份的基本摘要，如图 2-38 所示。如果选择的是以后执行方式，则系统会把这样一份备份计划文件存放起来，等到指定的时间执行。

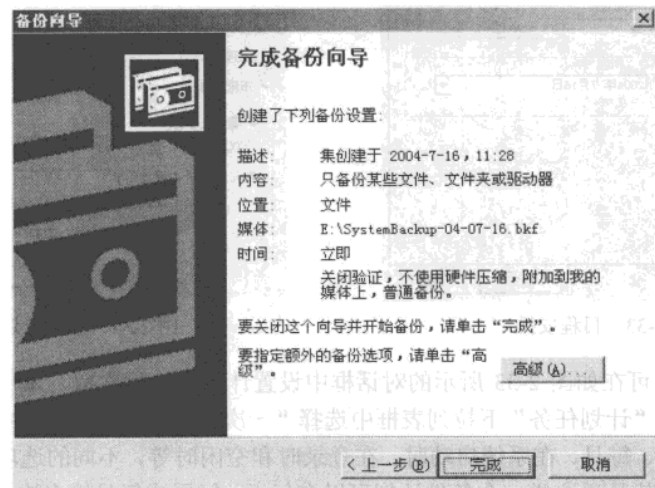


图 2-36 完成备份向导

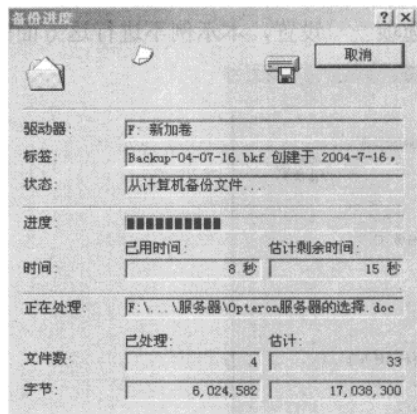


图 2-37 备份进度图

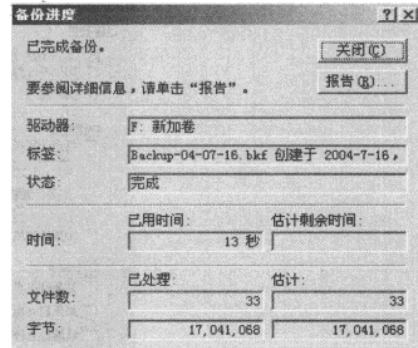


图 2-38 备份完成

第 3 章 服务器方面

本章的主要内容都是关于服务器管理的，在第一节中介绍了有关域的一些知识。如：怎样快速创建大量域用户、快速更改域名的方法等。接下来分别总结了服务器端问题解决的经验、客户端问题解决的经验。

在本章的后几节中又介绍了关于如何增强服务器功能的经验，使服务器提供更多更好的服务。在轻松管理服务器这一节中介绍几个简单而实用的小实验。在最后一节中给读者介绍了服务器安全管理的经验，为读者对服务器的安全管理提供参考。

3.1 AD 服务器方面的经验

在企业的域管理中，尤其是新建域以后，需要大批量的添加域用户，怎样才能迅速的添加大量的域用户呢？在公司需要更改域名的时候，如何能快速更改 Windows 域名呢？还有如何将一个已存在的域完整的迁移呢？本节将这几方面的经验总结跟读者一起分享。

3.1.1 快速创建大批量域用户的小技巧

在 j 市政府实习的时候，遇到了一个令人头疼的问题。为了保证 j 市政府的网络畅通，在给其改造网络时，决定其实现域管理，当把所有用户及账户收集来时头晕了——实在太多了。仔细思考之后，于是决定使用命令行快速建立所有用户的用户账号。对于规模较大的单位来说很可能遇到同样的问题，所以本节就介绍一下如何快速创建大批量域用户。

在这里，用户的批量导入是使用 csvde 这个命令行来完成的。由于需要使用命令行导入用户的账户信息，于是决定使用 XLS 文档对所有信息进行记录，以便于日后方便导入与修改。用户名及账户收集如表 3-1 所示。

表 3-1 用户名及账户收集

DN	objectClass	asmAccountName	userPrincipalName	displayName
CN=xxzx-1,OU=xxzx,DC=heuet,DC=com	User	xxzx-1	Xxzx-1@heuet.com	信息中心-黄磊
CN=xxzx-2,OU=xxzx,DC=heuet,DC=com	User	xxzx-2	Xxzx-2@heuet.com	信息中心-陈光
CN=xxzx-3,OU=xxzx,DC=heuet,DC=com	User	xxzx-3	Xxzx-3@heuet.com	信息中心-潘宁
CN=xxzx-4,OU=xxzx,DC=heuet,DC=com	User	xxzx-4	Xxzx-4@heuet.com	信息中心-李海

当然，光是这样的 XLS 文档肯定是不能对活动目录进行导入的，还需要做系统的准备工作才可以。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 1 步，建立 OU “xxzx”，如图 3-1 所示。

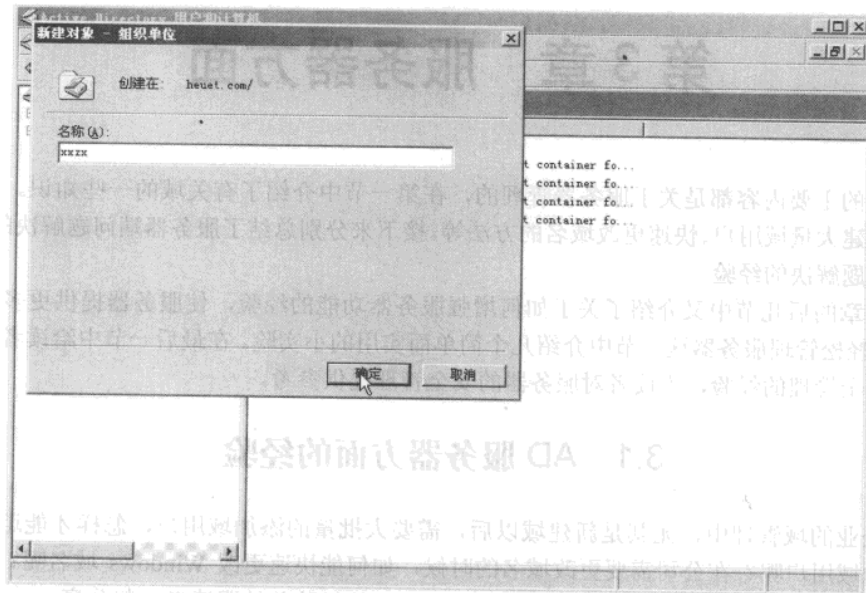


图 3-1 建立 “xxzx” OU

第 2 步，将 XLS 转存为 CSV 档案，如图 3-2 所示。

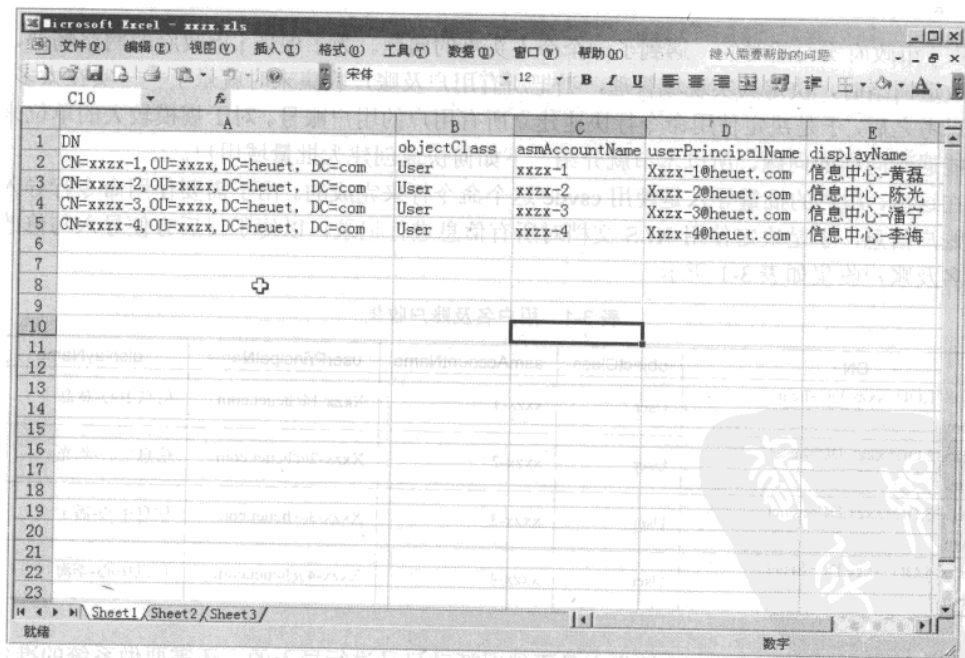


图 3-2 将 XLS 的文件转存为 csv 格式

第3步，在命令提示符下输入“csvde”命令，如图3-3所示，实现导入xxzx.csv文件的功能。



图 3-3 输入“csvde”命令

第4步，查看活动目录里“xxzx”有没有发生变化，来验证是否导入成功。

第5步，现在我们要将所有用户启用并设定相应的密码，还以xxzx这个OU为例，完成用户的导入工作。

案例中只有4个用户，实验环境中我们不可能为每个用户一个个设定密码，所以无法启用用户。此时我们可以修改注册表，使其允许用户为空密码，当然这只是为了更快的启用账户，随后我们可以设定让用户重启后设定密码。

3.1.2 快速更改公司 Windows 域名的方法

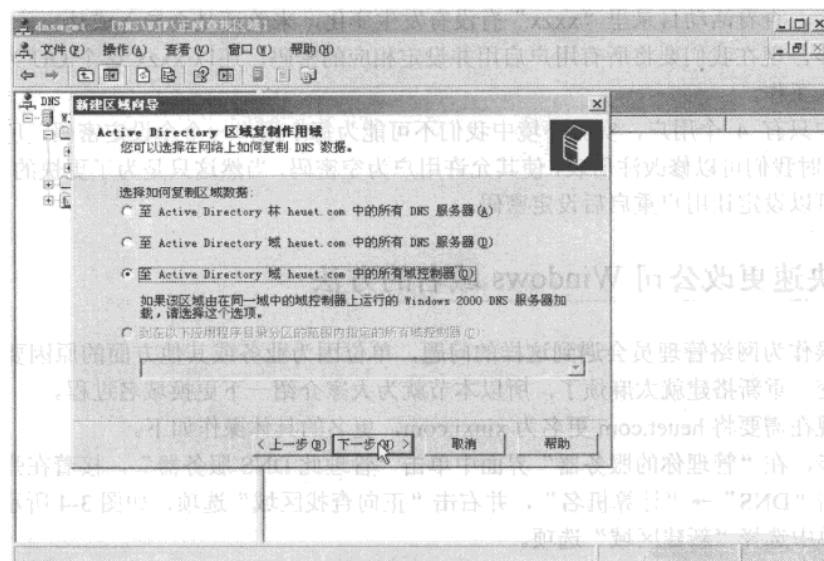
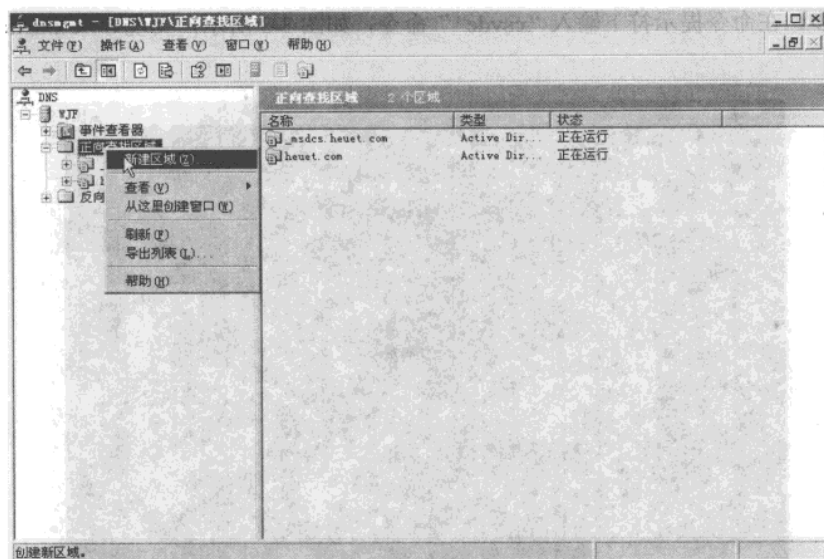
有时候作为网络管理员会遇到这样的问题，单位因为业务或其他方面的原因要改域名，而其他不变。重新搭建就太麻烦了，所以本节就为大家介绍一下更换域名过程。

假设现在需要将heuet.com更名为xinxi.com，更名的具体操作如下。

第1步，在“管理你的服务器”界面中单击“管理此DNS服务器”，接着在弹出的窗口中依次单击“DNS”→“计算机名”，并右击“正向查找区域”选项，如图3-4所示。在弹出的下拉菜单中选择“新建区域”选项。

第2步，打开“新建区域”向导，进入“区域类型”设置框并选择默认状态。在进入“Active Directory 区域复制作用域”对话框后，选择“至 Active Directory 域 heuet.com 中的所有域控制器”单选按钮，如图3-5所示。单击“下一步”按钮，在“区域名称”对话框中输入更改后的区域名称，如xinxi.com，接着单击“下一步”按钮，如图3-6所示。在“动态更新”设置框中选择默认状态完成设置。在完成上述操作后，就等于完成了目的域的建立。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第3步,在 Windows Server 2003 中,只有提升域、林的功能级别后,系统才会允许更改域名称,所以接下来应依次单击“开始”→“管理工具”→“Active Directory 域和信任关系”,在打开的窗口中右击“heuet.com”选项,在弹出的快捷菜单中选择“提升域功能级别”选项,如图 3-7 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

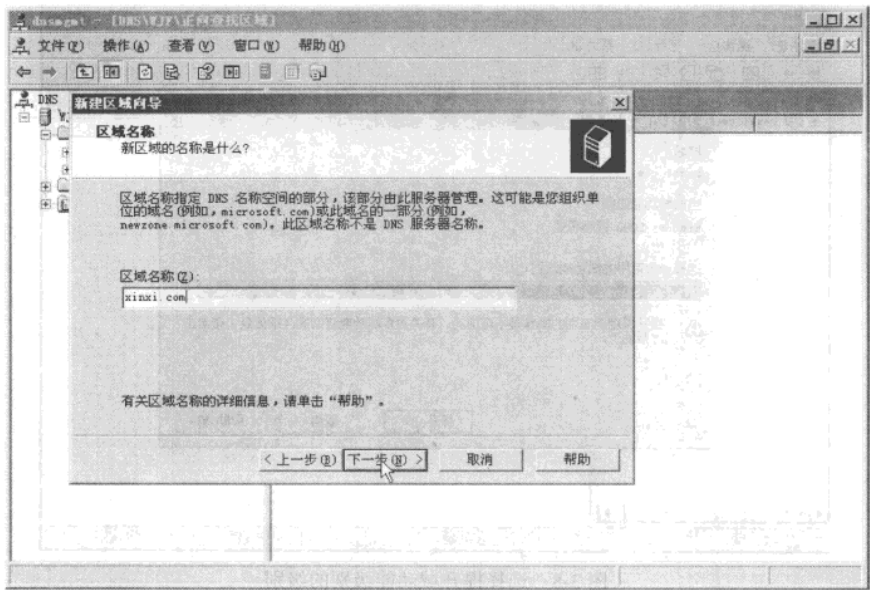


图 3-6 输入新域名称

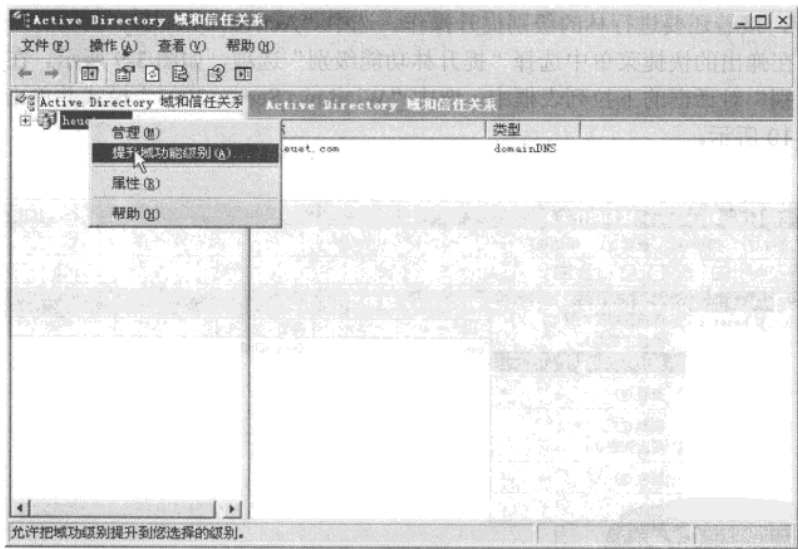


图 3-7 提升域功能级别

第 4 步，进入“提升域功能级别”对话框，单击“选择一个可用的域功能级别”下三角按钮，在弹出的下拉列表框中选择“Windows Server 2003”并单击下方的“提升”按钮，如图 3-8 所示。在弹出的提示框中单击“确定”按钮。在弹出级别提升成功的提示框后，单击“确定”按钮即可。

网管天下 网管经验谈

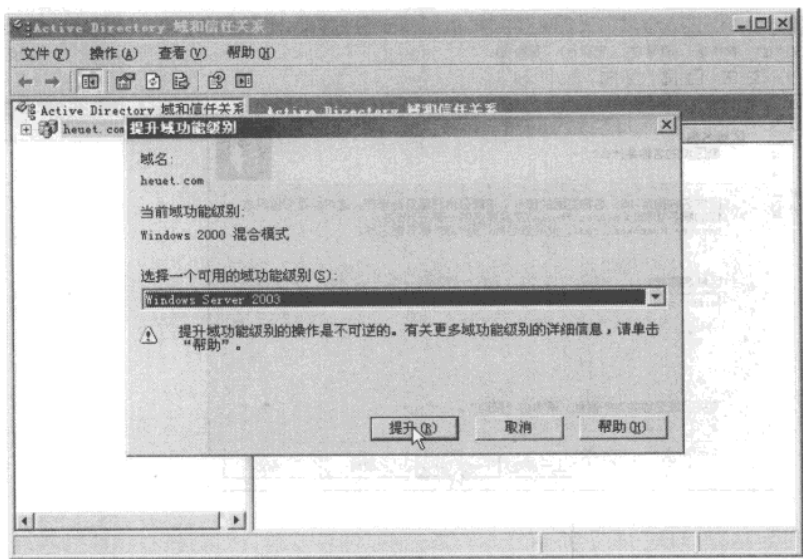


图 3-8 选择提升域功能级别的级别

第 5 步，接着还要进行林的级别提升操作。选中“Active Directory 域和信任关系”项并单击右键，在弹出的快捷菜单中选择“提升林功能级别”选项，如图 3-9 所示。在弹出的“提升林功能级别”对话框的下拉列表框中，选中“Windows Server 2003”模式并单击“提升”按钮，如图 3-10 所示。

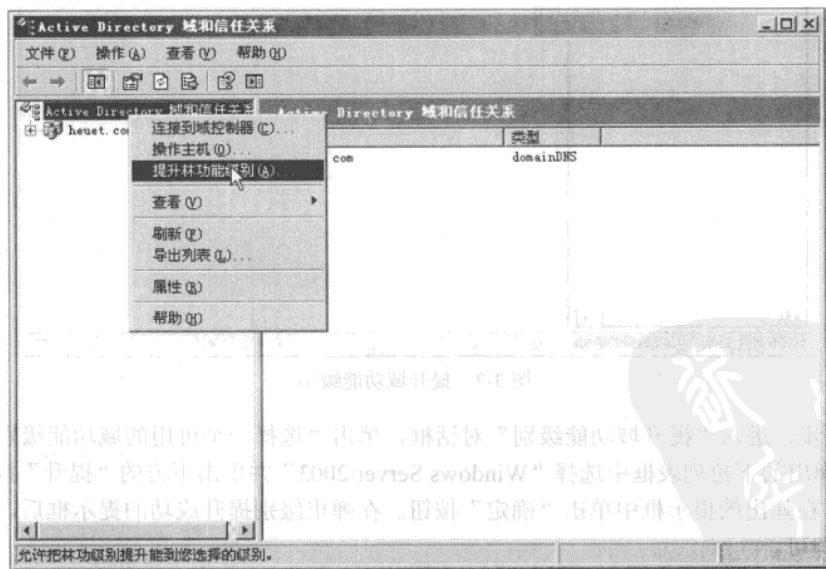


图 3-9 提升林功能级别

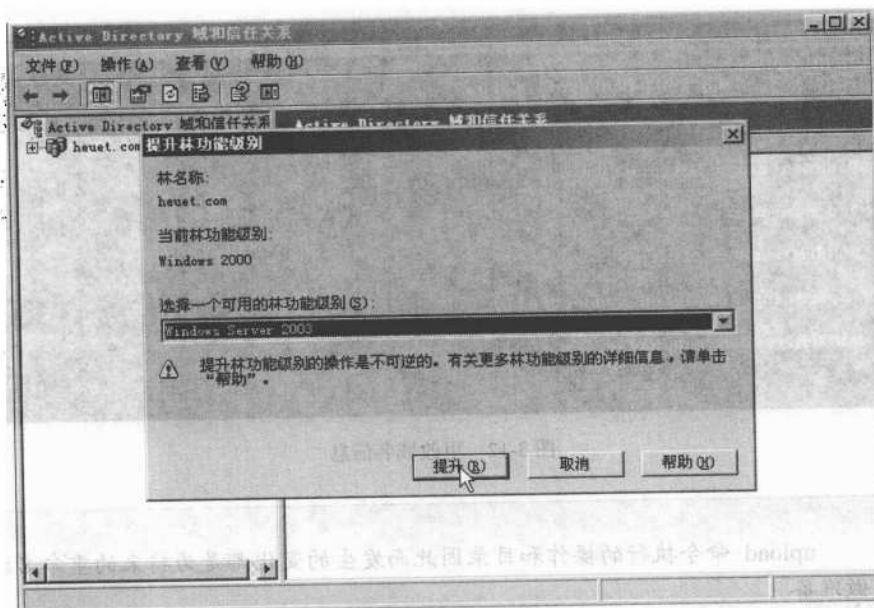


图 3-10 选择提升林功能级别的模式

第 6 步，做完准备工作后，现在就可以使用域更名工具“rendom”来完成域的更名了。把 Windows Server 2003 的安装光盘放入光驱，将“\VALUEADD\MSFT\MGMT”下的 DOMREN 目录复制到系统的 C 盘根目录下。接着在命令提示符窗口中进入 DOMREN 目录，输入“rendom /list”命令，如图 3-11 所示。该命令为当前林生成描述信息（将会使用 XML 编码结构把信息写入到一个输出文件中，默认文件名为 domainlist.xml）。

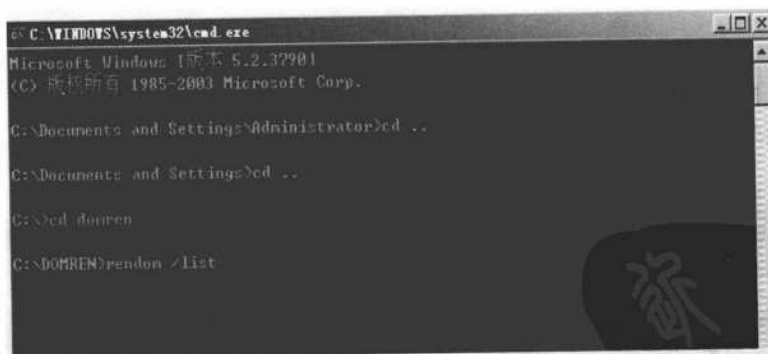


图 3-11 为当前林生成描述信息

第 7 步，用“记事本”对 domainlist.xml 文件进行编辑。将其中的“heuet.com”全部替换为新域的名称“xinxi.com”，再将 NetBIOS 的名称也进行相应的更换后，保存该文件。接着返回命令提示符窗口，在命令行中输入“rendom /upload”命令，如图 3-12 所示。

网管天下 网管经验谈

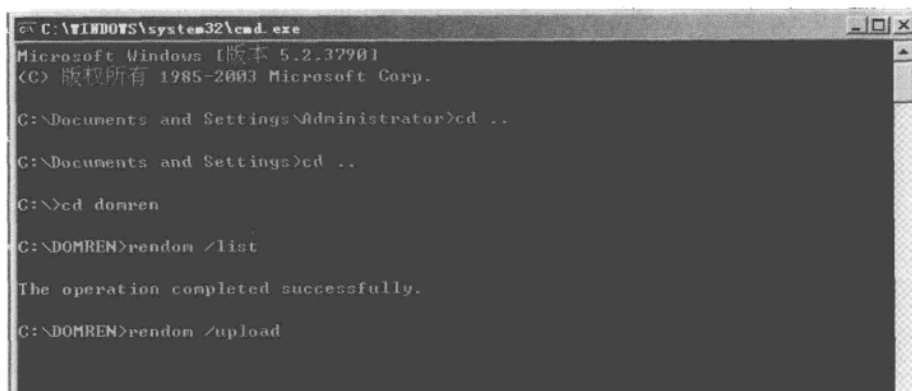


图 3-12 更改域名信息

注 意

upload 命令执行的操作和目录因此而发生的变化都是为将来的重命名操作做准备。

第 8 步，在命令提示符下输入“rendom /prepare”命令，如图 3-13 所示，实现校验连到该域的所有域控制器是否准备就绪的功能。如果出现“successfully”信息，则表示连接各域控制器成功。此外，本测试还检查每台域控制器进行授权的情况，以确定运行“rendom /prepare”命令的用户是否得到了授权执行重命名的指令。如果用户没有得到“写”授权，命令将会失败。如果成功，再在命令提示符下输入“rendom /execute”命令，如图 3-14 所示。实现发出正式更改域名的指令的功能。如果出现“Successfully”的信息，那么表示域的重命名过程成功完成了。

第 9 步，在上述命令执行完毕后，系统将会自动关闭并重启。此外域中所有计算机必须执行两次关机操作，第一次关机用于使新域成员资格生效，第二次关机则用于将计算机的 DNS 后缀自动转换为新域名称。

注 意

如果 DNS 后缀没有自动更改，可右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“计算机名”选项卡设置界面后，单击“更改”按钮并根据提示操作即可。

第 10 步，在完成域的重命名后，如果你还希望组策略中的相关设置能够继续得到应用，就需要在命令提示符窗口的命令行中输入如下命令“gpfixup /olddns:heuet.com /newdns:xinxi.com /oldnb:heuet/newnb:xinxi /dc:xinxi.com”，如图 3-15 所示。如果看到“Start fixing non-site group policy links”信息，则表示上述命令已经成功执行。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd ..
C:\Documents and Settings>cd ..
C:\>cd domren
C:\DOMREN>rendom /list
The operation completed successfully.
C:\DOMREN>rendom /upload
The operation completed successfully.
C:\DOMREN>rendom /prepare
```

图 3-13 校验域控制器的连接功能

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd ..
C:\Documents and Settings>cd ..
C:\>cd domren
C:\DOMREN>rendom /list
The operation completed successfully.
C:\DOMREN>rendom /upload
The operation completed successfully.
C:\DOMREN>rendom /prepare
Waiting for DCs to reply.
Waiting for DCs to reply.
wjf.heuet.com was prepared successfully
1 server contacted, 0 servers returned Errors
The operation completed successfully.
C:\DOMREN>rendom /execute
```

图 3-14 发出更改域名的指令

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \
C:\>cd domren
C:\DOMREN>gpfixup /olddns:heuet.com /newdns:xinxi.com /oldnb:heuet/newnb:xinxi /
dc:xinxi.com
```

图 3-15 继承原域的组策略

第 11 步，在命令提示符下输入“rendom /clean”命令，如图 3-16 所示。实现从 Active Directory 中删除原域名的功能。至此我们已经成功修改了域名。



图 3-16 删除原域名

3.1.3 AD 复制的经验小结

本节跟读者探讨一下 AD 的复制方面的经验，这里从 3 个方面跟读者谈一谈在 AD 复制方面的经验：站点内部的复制、站点间的复制和同域内复制的冲突。

AD 数据库分 4 个目录分区，如图 3-17 所示。在森林级别复制的是前两个分区，即架构分区和配置分区，而在域级别复制的是域分区。

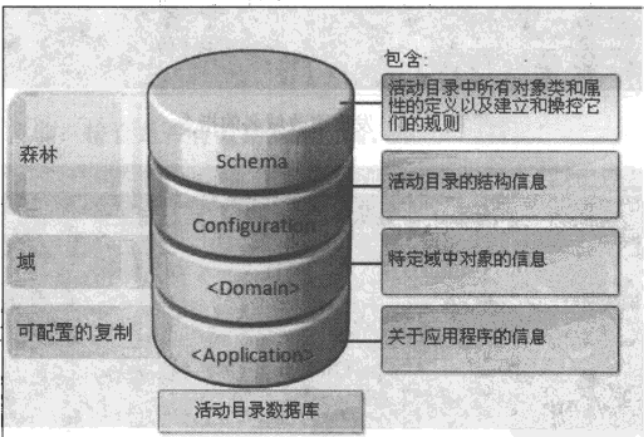


图 3-17 AD 数据库的 4 个主目录

1. 站点内部的复制

如果单域环境，同时存在多台 DC，此时每台 DC 都会同步森林及域级别的 3 个分区。如果多域环境，同时存在多台 DC，此时便会存在多路复制拓扑，如图 3-18 所示。图 3-18 中有 3 种复制拓扑，第一路是森林级别的复制，在所有的 DC 之间复制；第二路是域 A 的域分区的复制拓扑，在所有域 A 的 DC 之间复制；第三路是域 B 的域分区的复制拓扑，在所有域 B 的 DC 之间复制。如果图 3-18 中的 DC 之中还存在 GC，则上面的复制拓扑还会改变，因为 GC 是一个特殊的角色，它将拥有所有域的域分区对象及对象属性的子集。

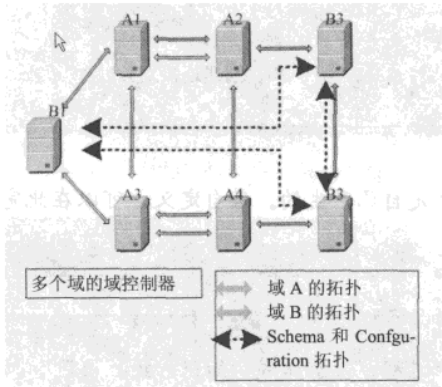


图 3-18 复制拓扑

其实复制拓扑是一个双向环（保证容错），而这个环是由每台 DC 上的 KCC 进程自动生成的。如果在图 3-18 中再加入新的 DC，KCC 会再次计算，生成新的环。当然自己也可以自定义，如图 3-19 所示。

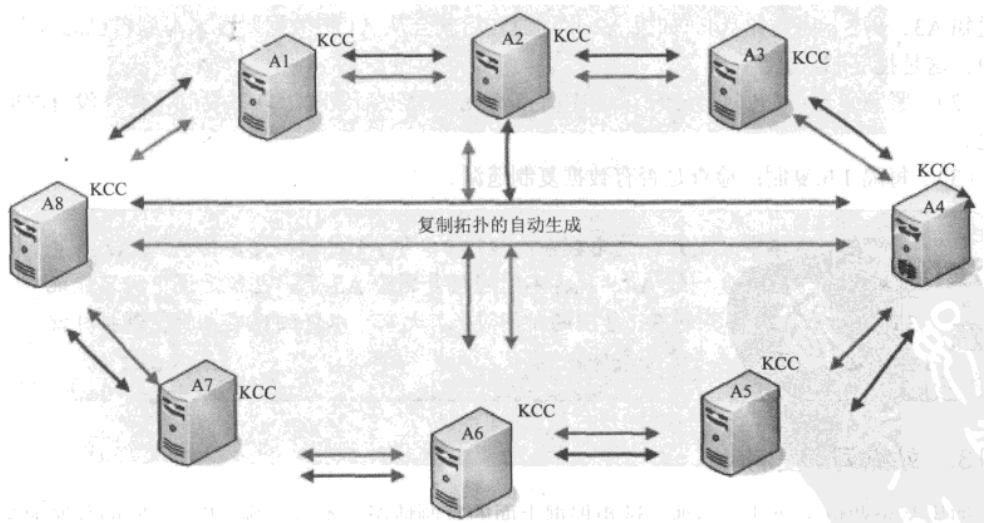


图 3-19 自动生成 KCC 进程

如果通过 KCC，在 A1 和 A2 之间创建一个连接对象，A2 就叫做 A1 的直接复制伙伴。如图 3-20 所示。

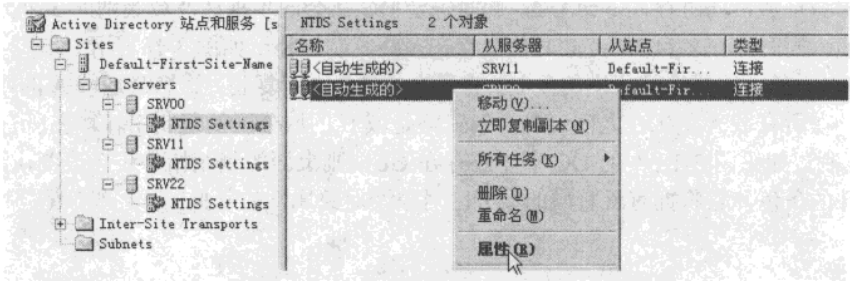


图 3-20 创建连接对象

注·意

这个连接对象是自己产生的。若自定义，可以在此完成。

说·明

KCC: 是一个进程，或翻译成“知识一致性校验”，它用来检查当前的 AD 环境，用于生成环形的复制拓扑。

2. AD 的复制有 3 种复制方式

- (1) 更改通知的方式：如果 A1 上创建了一个账号 pn，则它会 15 s 后通知 A2，然后 3 s 后通知 A3、再 3 s 后通知 A4。如果 A2 收到通知后就会从 A1 把数据要过来写到自己的数据库中。这是拉复制。
- (2) 紧急复制：如密码修改、账户锁定策略等。修改后就马上联系复制伙伴。没有时间延迟。
- (3) 每隔 1 h 复制：检查是否有数据复制遗漏。

注·意

在上述环中复制允许的路数不能超过 3，即 A1 把数据复制给 A2，A2 再复制给 A3，A3 再复制给 A4，就再不能间接复制给 A5 了，也就是说中间只能跳 3 跳。这个目的其实是不让复制的时间过长。大家可以仔细观察上面复制拓扑就会知道，它可以满足这个条件。

3. 站点间的复制

如果某企业位于两地或多地，试想根据上面的复制情况，不言而喻，DC 之间的复制流量很大，这个流量要跨越 WAN，这是不希望的。要控制复制，只能建站点，当然建站点的好处是可以控制用户的登录流量。这样便可以按计划进行 AD 的复制，同时这里复制还是压缩的，

基本上是原来流量的 15% 左右。站点内复制和站点之间复制的特点如图 3-21 所示。

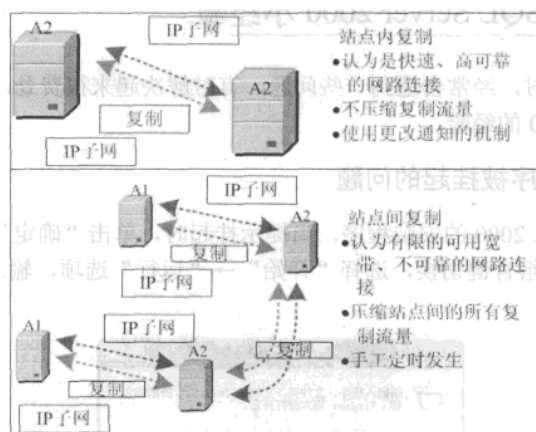


图 3-21 站点内和站点间复制的特点

4. 同域内复制冲突问题：有属性冲突、删除的容器冲突和 RDN 冲突

属性冲突：是指同一个对象的相同属性在两台 DC 上有所不同。

删除的容器冲突：在某个容器内添加对象或将对象转移到此容器内，但这个容器已经在另一个 DC 上被删除了。（在第一台 DC 上删除的容器还没有复制到这个 DC 之前）：此时该对象会被移动到一个叫 lostandfound 的容器中，这个容器你需要打开“高级”来查看到，你可以再把这个对象移到其他容器。

RDN 冲突：是指你在两台 DC 上建两个同名用户。在时间上后建的那个用户名会被改名，其实两个都存在。

属性值冲突的解决办法：会以戳值最高为优先，AD 会根据对象的属性戳（stamp）来解决冲突的问题，它包括 3 个数据，版本号：初始为 1，为最先比较者；修改时间：若版本号相同，此修改时间较后的优先；DC 的 GUID：若上修改时间相同，会比较 GUID，高的优先（Repadmin/showmeta DN 可以查看用户或 OU 的版本号）。

AD 的复制很重要，在企业里，如果控制不好，会造成域用户登录有问题或很慢。其实 AD 的复制主要复制的东西有两个：一是数据库本身的复制，二是 SYSVOL 之间的复制，而 SYSVOL 如果复制不成功，会造成组策略不生效。

3.2 服务器端问题解决经验

本节中介绍了服务器端常见的一些问题的解决和日常的一些网络维护经验。例如，WSUS 服务问题的解决方法，Windows Vista 的远程部署、发布内网 FTP 服务器等问题的经验。所有的这些都是建立在服务器端的一些服务，要保证局域网的正常运行，首先要保证所有的服务能够正常提供给客户端。

3.2.1 关于安装 SQL Server 2000 小经验

在安装 SQL2000 时，经常会遇到一些问题，有时解决起来很费劲。本节就给大家介绍一些安装 SQL Server 2000 的经验。

1. 提示安装程序被挂起的问题

第 1 步，运行 SQL 2000 的安装程序，当提示挂起时，单击“确定”按钮，注意不要退出安装程序，用 Alt+Tab 组合键切换，选择“开始”→“运行”选项，输入“regedit”，打开注册表，如图 3-22 所示。

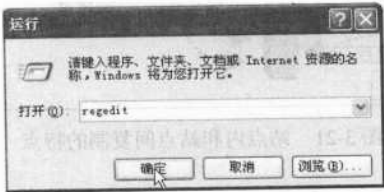


图 3-22 打开注册表

第 2 步，找到目录 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager，如图 3-23 所示。



图 3-23 找到 Session Manager

第 3 步，删除其中的“PendingFileRenameOperations”（在这里说明一下，PendingFileRenameOperations 文件位于 Session Manager 右侧，即单击 Session Manager 时，在右边就可以看到了）如图 3-24 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

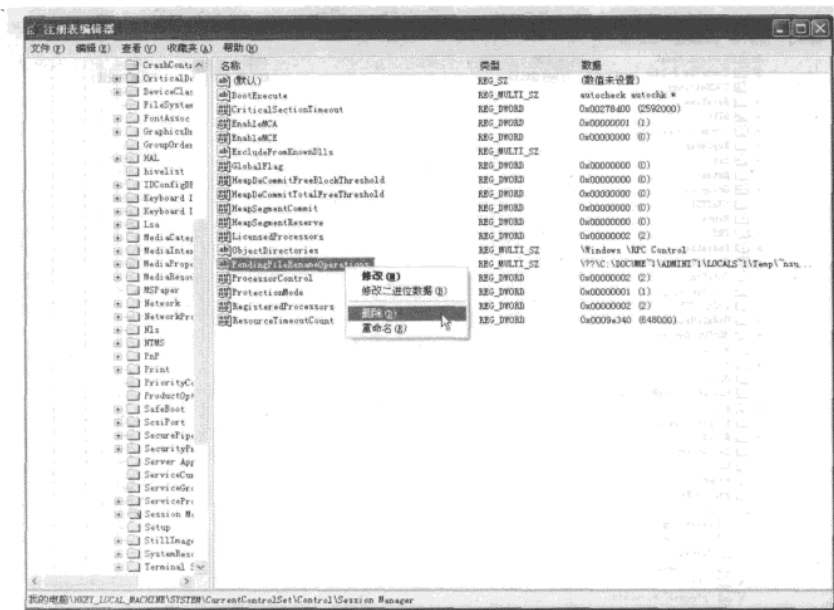


图 3-24 删除 PendingFileRenameOperations

第 4 步，关闭注册表，重新开始安装 SQL Server 2000，问题就解决了。

2. 安装程序配置服务器失败

参考服务器错误日志和 C:\WINNT\sqlstp.log 了解更多信息。
WINNT 目录下的 sqlstp.log 中最后是这样的错误信息：

```
正在启动？
Chinese_PRC_CI_AS
-rm -Q -T4022 -T3659
正在与服务？
driver={sql server};server=GH;UID=sa;PWD=;database=master
[Microsoft][ODBC SQL Server Driver][Shared Memory]一般性网络错误。
[Microsoft][ODBC SQL Server Driver][Shared Memory]ConnectionRead (recv()).
driver={sql server};server=GH;UID=sa;PWD=;database=master
[Microsoft][ODBC SQL Server Driver][Shared Memory]一般性网络错误。
[Microsoft][ODBC SQL Server Driver][Shared Memory]ConnectionRead (recv()).
driver={sql server};server=GH;UID=sa;PWD=;database=master
[Microsoft][ODBC SQL Server Driver][Shared Memory]一般性网络错误。
[Microsoft][ODBC SQL Server Driver][Shared Memory]ConnectionRead (recv()).
SQL Server 配置？
```

第 1 步，把安装目录和 C:\Program Files 下的 Microsoft SQL Server 文件夹删除，删除在 current_user 和 local_machine\software\microsoft\ 下有关 Microsoft SQL server 全部信息。

第 2 步，打开注册表，然后打开 HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft \Windows\CurrentVersion\Setup\ExceptionComponents，如图 3-25 所示。

网管天下 网管经验谈



图 3-25 找到“ExceptionComponents”

第 3 步，将 ExceptionComponents 下面的文件夹全部删除。

第 4 步，重新启动，重新安装 SQL Server 2000，问题得到解决。

3.2.2 Windows Vista 自动远程部署经验

Windows 部署服务是 RIS(远程安装)服务的升级版本，它可以使用“Windows 映像(WIM)文件”安装 Windows 操作系统。目前，Windows 映射文件格式包括 Windows Vista 和 Windows Server 2008 操作系统。也就是说，Windows 部署服务可用于远程安装 Windows Vista 和 Windows Server 2008 操作系统。

Windows 部署服务包含 PXE 服务器和普通文件传输协议(TFTP)服务器。此外，Windows 部署服务还包含客户端界面和管理单元。Windows 部署服务组件包括“服务器组件”、“客户端组件”和“管理组件”。Windows 部署服务将使部署 Windows 操作系统的用户获得如下好处：

- (1) 比手动安装更有效率。
- (2) 提高操作系统和应用程序的性能一致性。
- (3) 与手动安装相比，减少了对咨询台的呼叫。
- (4) 减少用户安装新操作系统和常用应用程序所需的时间。

Windows 部署服务使用 Windows 预安装环境(Windows PE)提供客户端启动服务。Windows 部署服务客户端使用 Windows PE 提供的菜单，并且与安装 Windows 的步骤相同。

在服务器或者客户端计算机，Windows 部署服务对内存或 CPU 速度都没有额外的要求。Windows 部署服务服务器需要使用 NTFS 分区，必须为存储映像文件提供足够的磁盘空间。

服务器方面 3

Windows 部署服务要求采用 Windows Server 2003 操作系统，安装 SP1 或 SP2 的 Windows 部署服务更新包，并安装远程安装服务（RIS），但无需对其进行配置。（如果已安装 RIS，Windows Server 2003 SP2 将默认安装 Windows 部署服务。）

Windows 部署服务的环境必须满足下列要求：

- (1) Windows 部署服务服务器必须是 Active Directory 域的成员。
- (2) 必须安装 DHCP 服务器。
- (3) 具有使用 PXE 启动的计算机。

安装配置 Windows 部署服务的具体步骤如下：

第 1 步，以管理员账户登录到服务器，在“添加/删除程序”中运行“添加删除 Windows 组件”。进入“Windows 组件向导”页面，在“Windows 组件”页中，选中“Windows 部署服务”，如图 3-26 所示，实现安装该组件的功能。

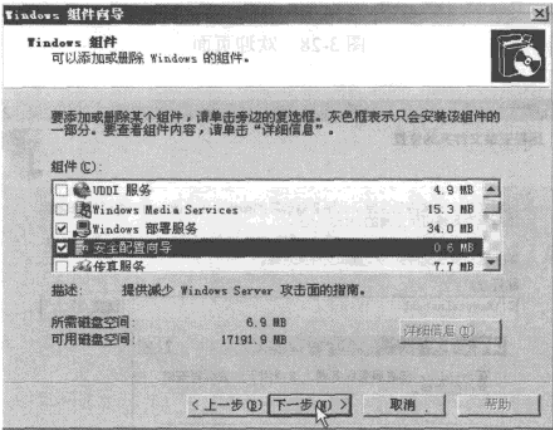


图 3-26 安装“Windows 部署服务”组件

说明 如果 Windows Server 2003 不是集成“SP2”安装的，还会提示插入 Windows Server 2003 的安装光盘或者 Windows Server 2003 SP2 的安装光盘。请根据提示，放入相应的光盘。安装完成后，按照提示，重新启动计算机。

第 2 步，从“管理工具”中运行“Windows 部署服务”，打开“Windows 部署服务”窗口。用鼠标右键单击域名称，在弹出的快捷菜单中选择“配置服务器”选项，如图 3-27 所示。运行“Windows 部署服务配置向导”在欢迎页面单击“下一步”按钮，如图 3-28 所示。在“远程安装文件夹的位置”对话框中，选择大小适用的 NTFS 分区，作为 Windows 部署服务保存操作系统映像的位置，如图 3-29 所示。

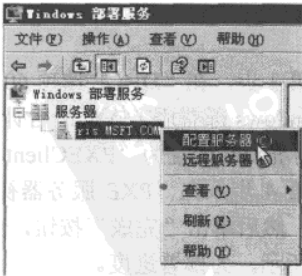


图 3-27 配置服务器

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

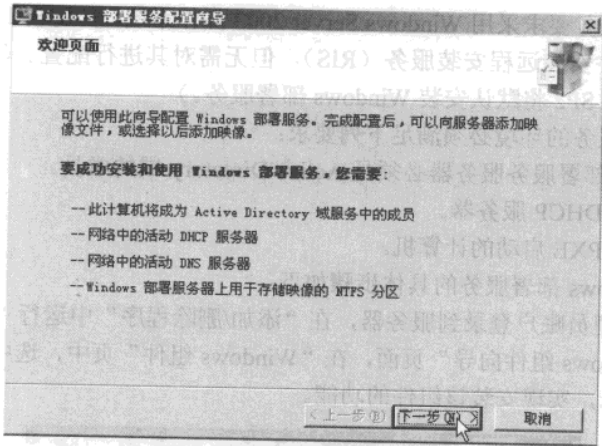


图 3-28 欢迎页面

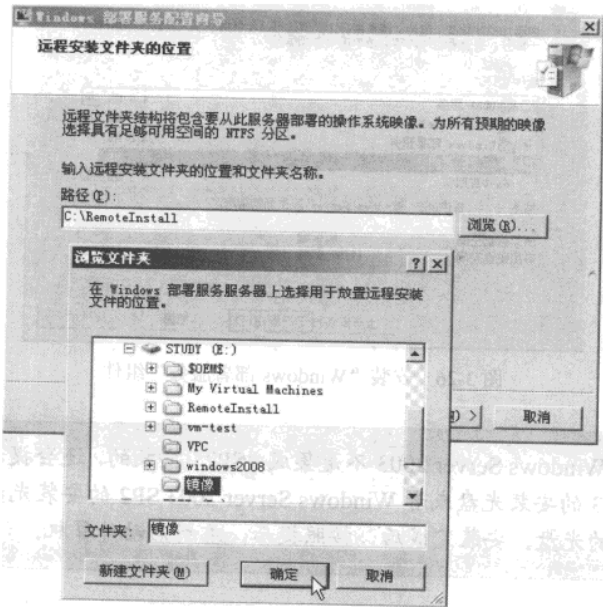


图 3-29 选择安装路径

第 3 步，在“DHCP 选项 60”页面中，配置 DHCP 服务器。如果网络中的 DHCP 服务器与 Windows 部署服务在同一台计算机上，请选中“不侦听端口 67”复选框并选中“将 DHCP 选项标记#60 配置为 ‘PXEClient’”复选框，如图 3-30 所示。

第 4 步，在“PXE 服务器初始设置”页面中，选择“不响应任务客户端的计算机”单选按钮，然后单击“完成”按钮，如图 3-31 所示。开始配置 Windows 部署服务服务器，如图 3-32 所示，为部署进度。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

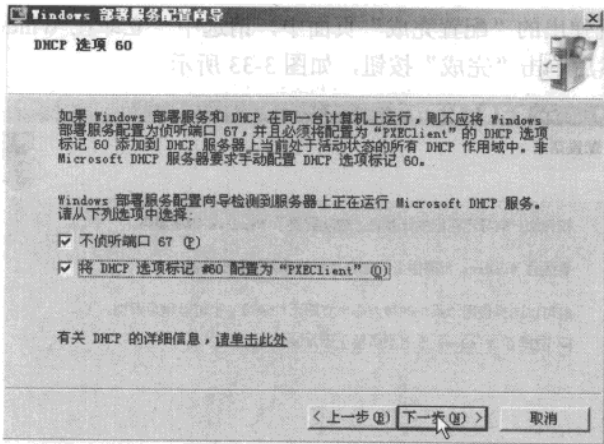


图 3-30 DHCP 选项 60

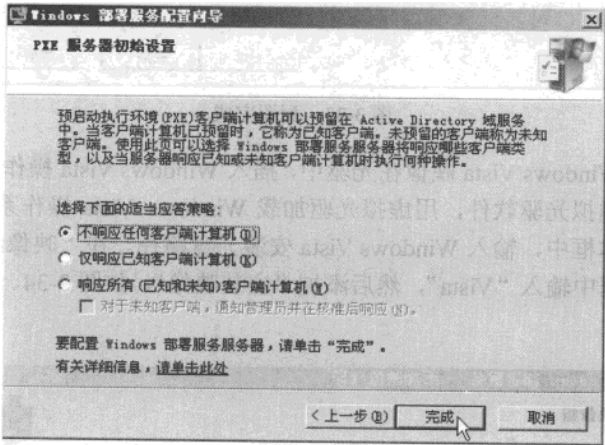


图 3-31 PXE 服务器初始设置

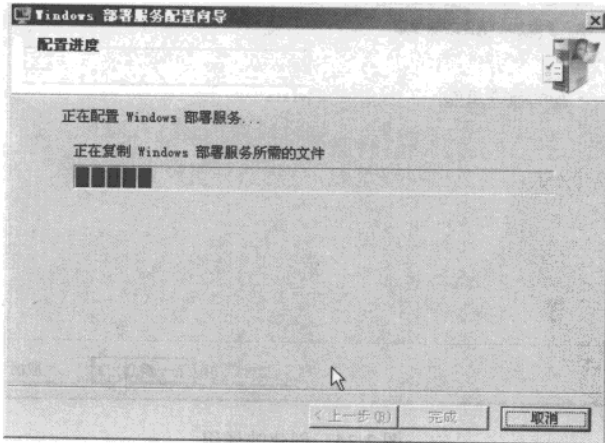


图 3-32 部署进度

网管天下 网管经验谈

第 5 步，在系统弹出的“配置完成”页面中，请选中“立即在 Windows 部署服务器上添加映像”复选框，然后单击“完成”按钮，如图 3-33 所示。

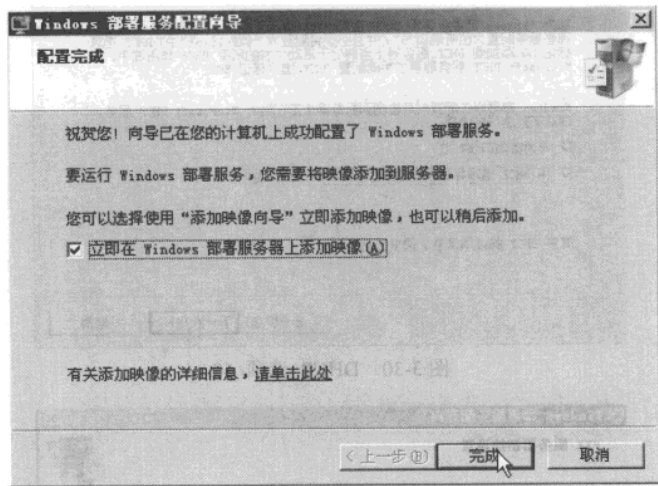


图 3-33 配置完成

第 6 步，添加 Windows Vista 映像。在光驱中，插入 Windows Vista 操作系统的安装光盘（或者在服务器上安装虚拟光驱软件，用虚拟光驱加载 Windows Vista 操作系统安装光盘映像），同时在“路径”文本框中，输入 Windows Vista 安装光盘路径。在“映像组”页面中，在“创建新映像组”文本框中输入“Vista”，然后添加“安装映像”，如图 3-34、图 3-35 和图 3-36 所示。

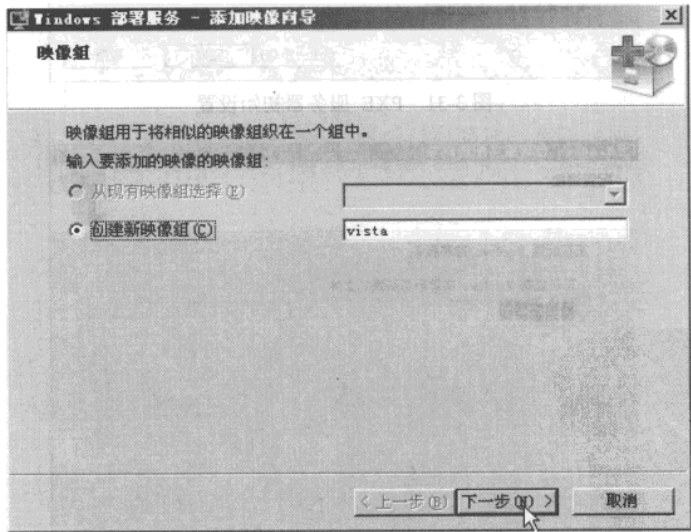


图 3-34 创建映像组

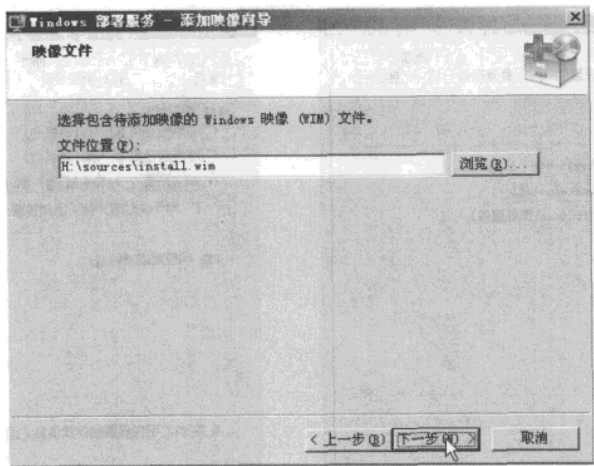


图 3-35 添加映像文件

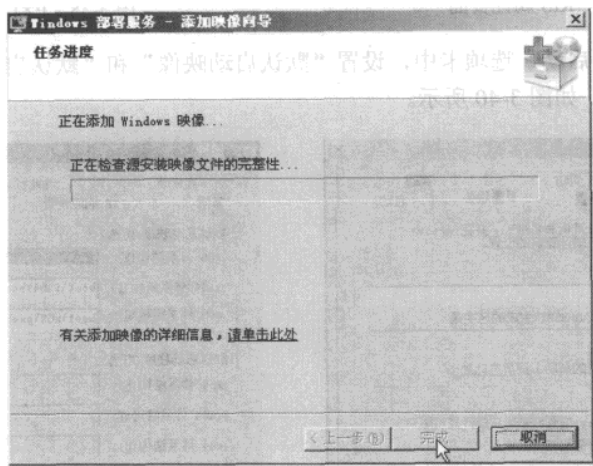


图 3-36 添加安装映像

第 7 步，添加完安装映像与启动映像后，用鼠标右键单击域名，从快捷菜单中选择“属性”，打开“RIS 属性”页面，如图 3-37 所示。

第 8 步，在“PXE 响应设置”选项卡中，选中“响应所有（已知和未知）客户端计算机”单选按钮，如图 3-38 所示。

第 9 步，在“目录服务”选项卡的“新建客户端命名策略”选项组中，设置客户端计算机的命名原则。在“客户端账户位置”选项组中，设置使用 Windows 部署服务的客户端账户的位置，如图 3-39 所示。在以前的 RIS 远程安装服务器中，使用 RIS 部署的计算机只能保存在 Active Directory 的“Computers 容器”中，而在 Windows 部署服务中，使用 Windows 部署服务安装操作系统的计算机可以统一保存在一个“容器”中。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

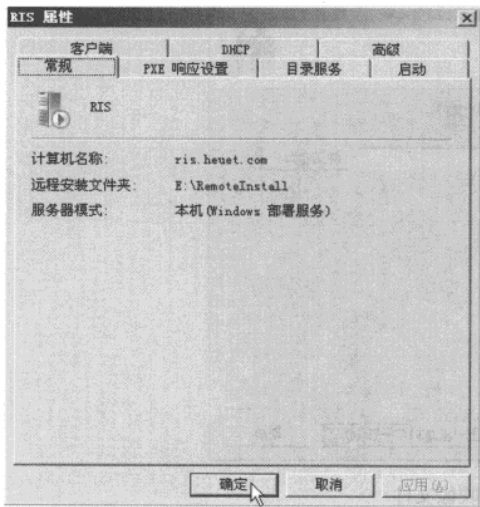


图 3-37 RIS 属性页面

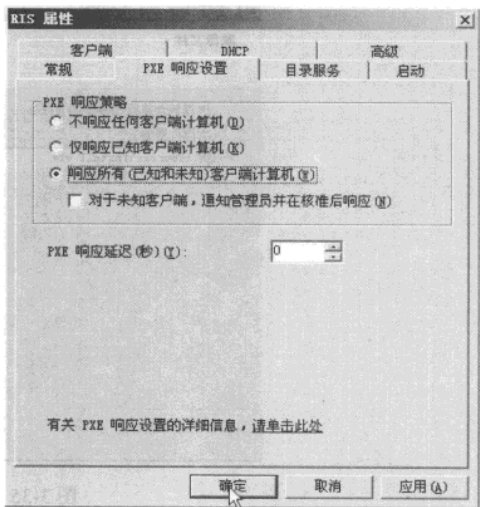


图 3-38 PXE 响应策略

第 10 步，在“启动”选项卡中，设置“默认启动映像”和“默认启动程序”选项组，通常选择默认值即可，如图 3-40 所示。

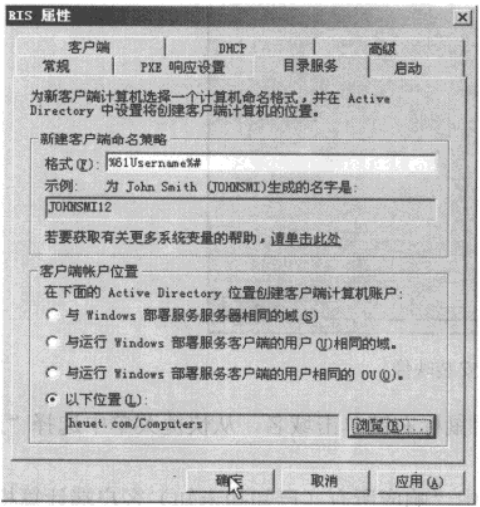


图 3-39 设置目录服务

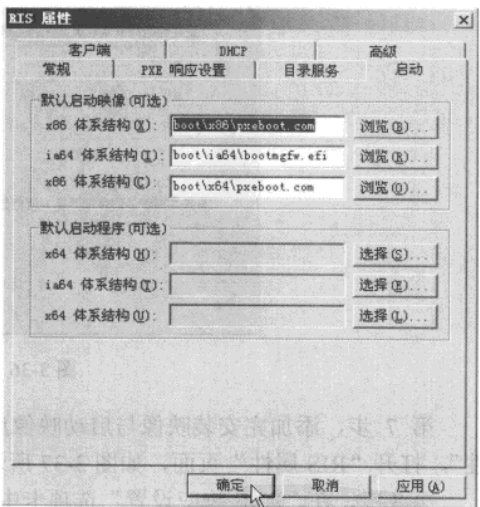


图 3-40 设置启动选项卡

第 11 步，在“高级”选项卡中，选择“允许 Windows 部署服务动态发现有效的 Active Directory 服务器”单选按钮和是否对 DHCP 服务器授权中选中“是，我想在 DHCP 中授权 Windows 部署服务服务器”单选按钮，如图 3-41 所示。

第 12 步，在“DHCP”选项卡中，设置 DHCP 服务，如图 3-42 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

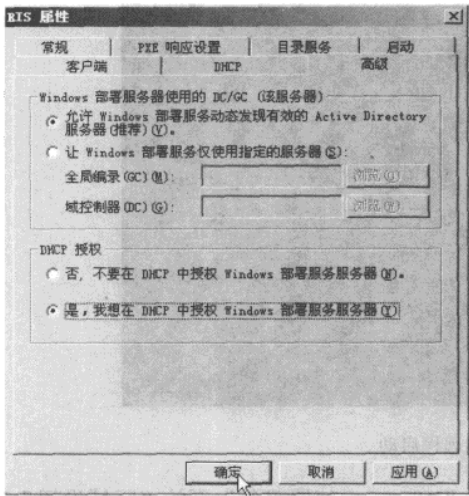


图 3-41 设置高级选项卡

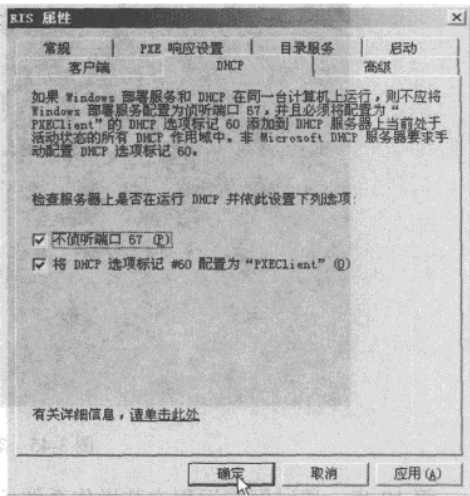


图 3-42 设置 DHCP 服务

第 13 步，在“客户端”选项卡中，设置是否启用无人参与文件，如图 3-43 所示。

第 14 步，打开 Active Directory 用户和计算机，为 Windows 部署服务创建一个账户，然后“委派”这个用户将计算机加入到域的权限，如图 3-44 所示。

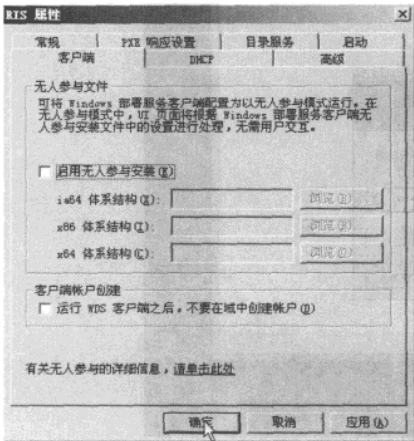


图 3-43 设置客户端

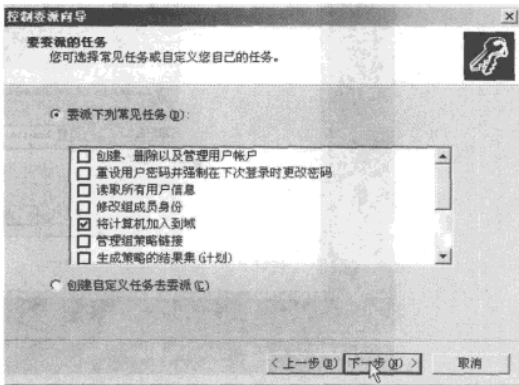


图 3-44 委派任务设置

第 15 步，选择一台网络中的计算机（这台计算机的硬件须满足安装 Windows Vista 的最低配置），进入 CMOS 设置，设置为“网卡最先引导”，然后重新启动计算机。

第 16 步，使用网卡启动后，当前计算机会从 DHCP 服务器获得地址，随后从 Windows 部署服务加载启动映像。按照屏幕提示，按 F12 键，如图 3-45 所示，开始加载启动映像并安装。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

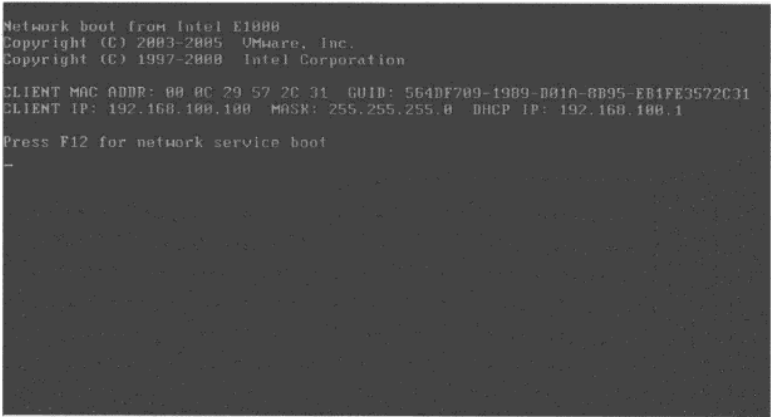


图 3-45 客户端远程启动

第 17 步，通过网络远程安装操作系统后，在“Windows 部署服务”页的“区域设置”选项中选择“中文（中国）”，在“输入和输入方法”中选择“中文简体”，然后根据系统提示输入用户名和密码，如图 3-46 所示。

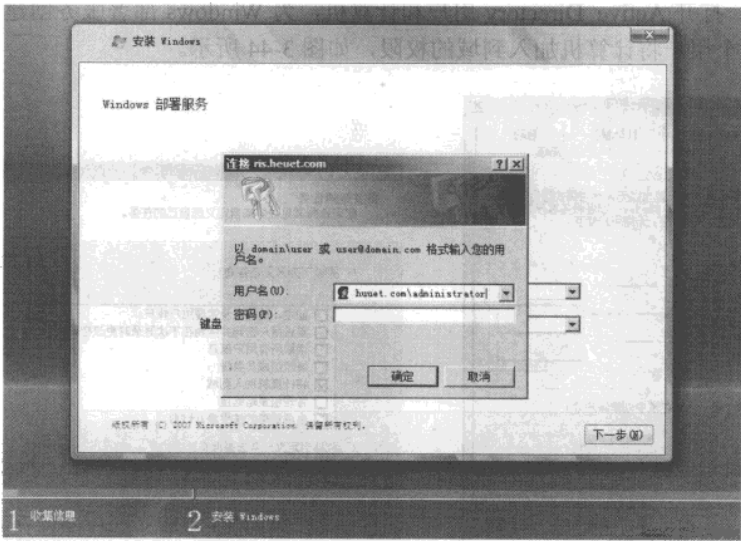


图 3-46 使用授权用户安装

第 18 步，在“安装 Windows”页中，选择要安装的操作系统，本例中就一个版本，所以就选默认的就以，如图 3-47 所示。

第 19 步，在“你想将 Windows 安装在何处”页中，选择安装 Windows Vista 的磁盘分区，如图 3-48 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

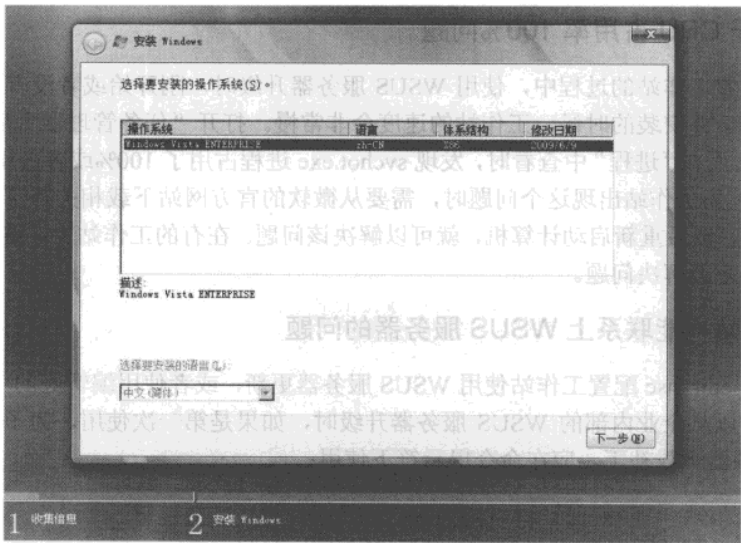


图 3-47 选择操作系统的版本

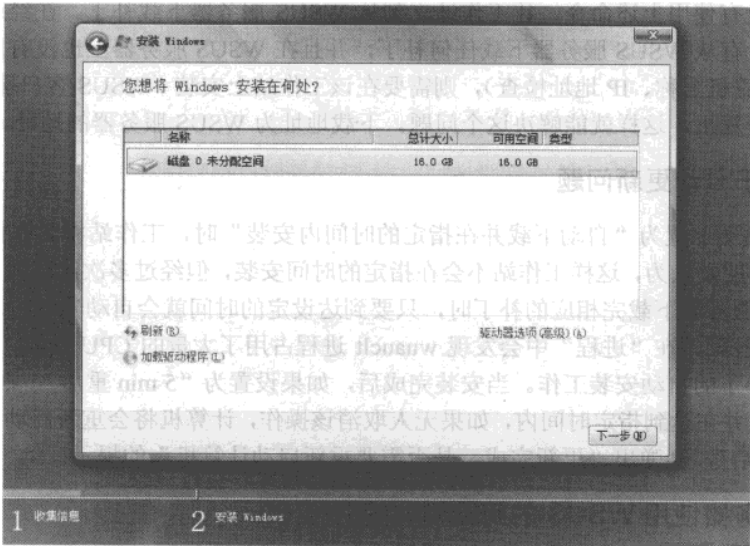


图 3-48 选择磁盘

以上设置完成后，Windows Vista 开始安装，在 15~20 分钟后，系统提示重新启动计算机以进入下一步。下面的安装过程与安装 Windows Vista 类似，本节不再赘述。

3.2.3 解决 WSUS 服务器的几个问题的经验

大多数网络管理员都有使用 WSUS 服务器的经验，本节就介绍一下使用 WSUS 时经常遇到的一些问题和作者自己总结的几条小经验。

网管天下 网管经验谈

1. 关于 CPU 占用率 100%问题

近期在配置工作站的过程中，使用 WSUS 服务器升级时，刚开始或者没有完全从 WSUS 下载所有的补丁并安装的时候，工作站的速度会非常慢。打开“任务管理器”后，显示 CPU 占用率 100%，而在“进程”中查看时，发现 `svchot.exe` 进程占用了 100%或者占用了将近 100% 的 CPU 资源，当工作站出现这个问题时，需要从微软的官方网站下载相关补丁，在工作站上安装这个补丁，然后重新启动计算机，就可以解决该问题。在有的工作站上，需要反复多次安装这个补丁，才能解决问题。

2. 工作站不能联系上 WSUS 服务器的问题

当使用 `gpedit.msc` 配置工作站使用 WSUS 服务器更新，或者使用编辑好的“注册表文件”导入工作站，以从企业内部的 WSUS 服务器升级时，如果是第一次使用，为了让工作站立刻从 WSUS 服务器下载补丁，应在命令提示符下使用：

```
Wuaucit /detectnow  
Wuaucitl /detectnow
```

之后，再使用“`netstat -an`”时，没有发现到 WSUS 服务器的连接。

或者，没有使用上述命令，让工作站立刻从 WSUS 服务器下载补丁。在经过几天之后发现，工作站没有从 WSUS 服务器下载任何补丁，并且在 WSUS 服务器上也没有发现该工作站（可以通过计算机名称、IP 地址检查），则需要在该工作站上安装“WSUS 客户端代理”程序，并重新启动计算机，这样就能解决这个问题。下载地址为 WSUS 服务器的地址。

3. 关于自动更新问题

当工作站端配置为“自动下载并在指定的时间内安装”时，工作站将会在指定的时间安装。可能有的朋友认为，这样工作站不会在指定的时间安装，但经过多次测试后发现，当工作站从 WSUS 服务器下载完相应的补丁时，只要到达设定的时间就会自动安装。这时，如果打开“任务管理器”，在“进程”中会发现 `wuaucit` 进程占用了大量的 CPU 资源，而该 `wuaucit` 进程会完成补丁的自动安装工作。当安装完成后，如果设置为“5 min 重启”，则会出现 5 min 倒计时窗口，并在达到指定时间内，如果无人取消该操作，计算机将会重新启动。如果没有配置“5 min 重启”，会弹出“更新完成，是否需要重新启动计算机”的提示。

4. 服务器使用 WSUS 的问题

对于 Windows Server 2008、Windows Server 2003 的服务器来说，最好设置服务器在夜间自动安装并自动重启，设置关键点为：在下班时间，不会影响正常工作。

5. 关于 Vista 客户端的问题

当工作站是 Vista 操作系统时，除了可以使用 `wuaucit` 命令立刻从 WSUS 服务器检查并下载补丁，还可以在“控制面板→Windows Update”中，单击“检查更新”按钮，立刻从 WSUS 服务器检查并下载更新补丁；如果 WSUS 服务器不能使用，可以单击“检查更新”按钮从 Microsoft 网站检查升级补丁，如图 3-49 所示。

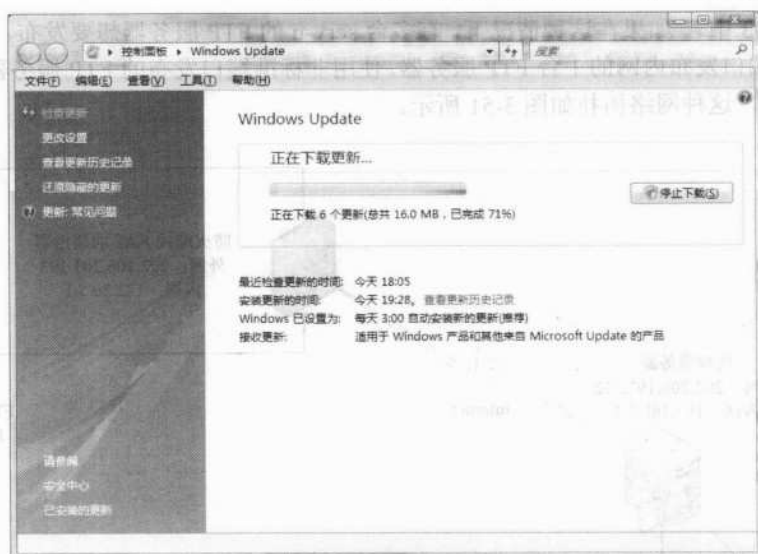


图 3-49 检查更新

6. 关于 Windows XP SP3 补丁的问题

在 WSUS 服务器上，Windows XP SP3 补丁不能自动“审批”，需要管理员在 WSUS 服务器上，手动审批该补丁。

7. 安装 XP SP3 后，出现错误代码：0x80070002

在安装 Windows XP 的 SP3 后，再次进入计算机后，提示“Windows 产品激活，一个问题阻止 Windows 正确检查此计算机的许可证。错误代码：0x80070002”，按了确定后又退回到错误提示，如此反复。这是由于缺少 C:\WINDOWS\system32\oembios.bin 文件造成的，主要原因是原来的 XP 是盗版的，或者虽然是正版的，但产品的激活码已经泄露，Microsoft 屏蔽了该号码。解决办法：重新安装操作系统；或者从能启动的计算机中，复制 oembios.bin 文件到出现错误的计算机中。

3.2.4 发布内网中多台 FTP 服务器的经验

许多网管可能都有这样的经验：在有一个公网 IP 地址的时候，如果内网有多台 FTP 服务器需要发布，除了其中的一台 FTP 服务器可以 21 端口发布，其他的 FTP 服务器只能使用 21 之外的端口进行发布。这样发布的 FTP 服务器，如果最终用户是内网用户（就是通过代理服务器或者 NAT 路由器共享上网的用户），在访问非标准端口的 FTP 服务器时，只能使用 PORT 模式，并且这些用户只能使用专门的 FTP 客户端软件如 FlashGet、CuteFTP 等，而不能使用 IE 等软件上传和下载。这种网络拓扑如图 3-50 所示。

如果 FTP 服务器具有更加复杂的网络，例如，一个 ISA Server 2006 具有公网地址 202.206.203.193，还有一个电信的出口。因为从公网访问该服务器的地址是很慢的，其网络中心又提供了一个公网地址 124.xx.xx.126，并且将这个地址映射到 ISA Server 公网地址

网管天下 网管经验谈

202.206.203.193 中。如果在这种情况下，有多台 serv-u 的 FTP 服务器想要发布，普通的方法，只能使用 21 端口发布内网的 1 台 FTP 服务器，使用非标准端口发布的 FTP 服务器是不能让公网用户访问的。这种网络拓扑如图 3-51 所示。

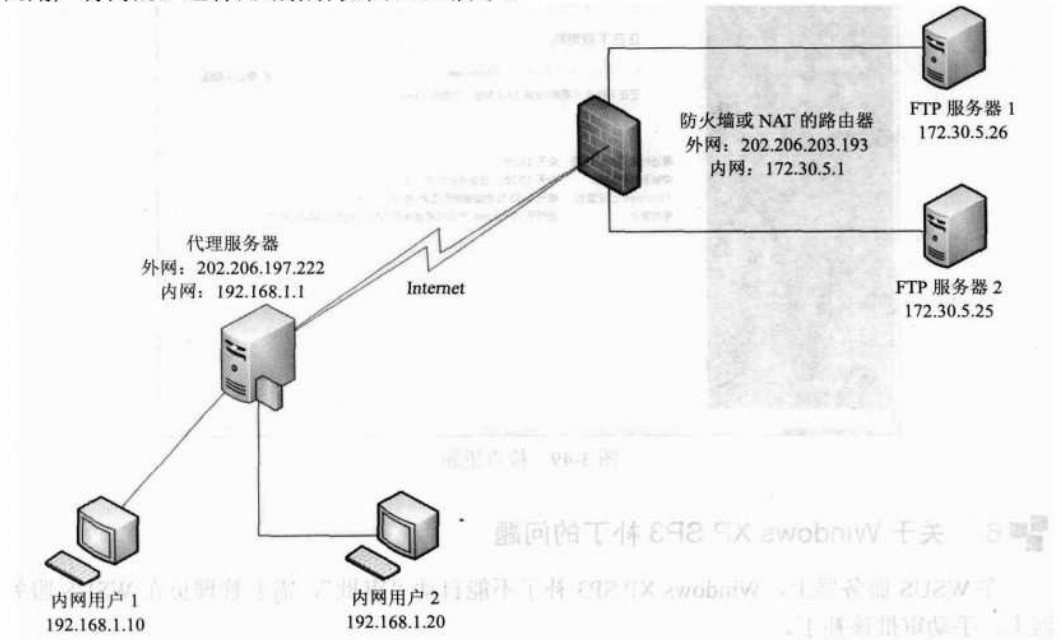


图 3-50 普通用户只能使用 PORT 模式访问非标准端口的 FTP 服务器

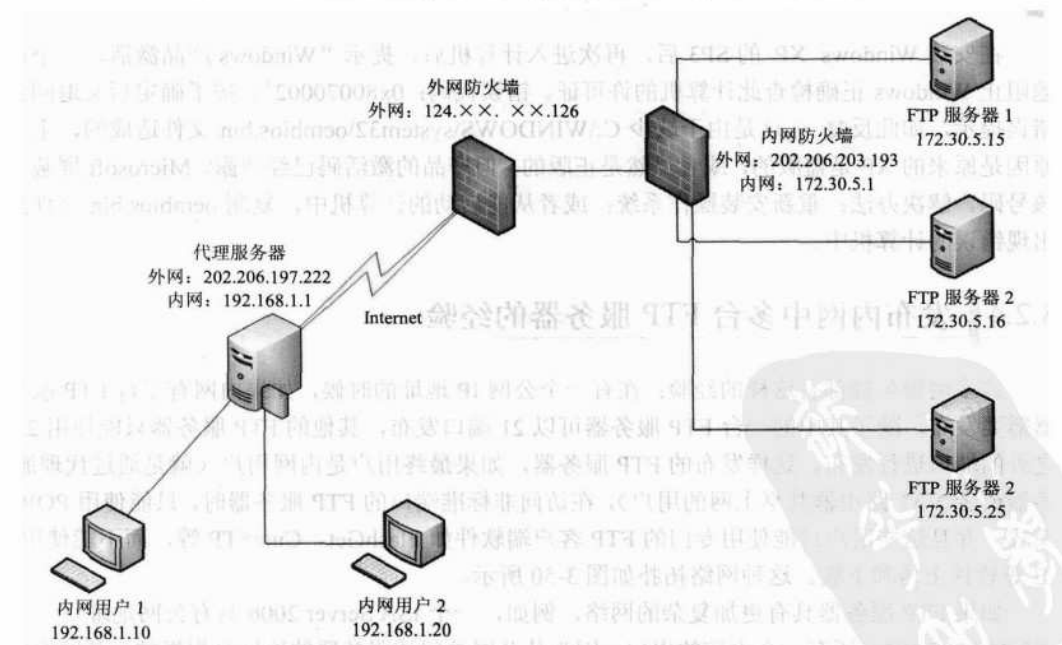


图 3-51 拓扑图

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

内网的防火墙以 ISA Server 2004 为例、内网的 FTP 服务器以 Serv-U 为例说明。该问题解决的关键点在于：

- (1) 为 Serv-U 指定 PASV 服务的 IP 地址。
- (2) 为 Serv-U 指定 PASV 服务的端口号。
- (3) 如果是使用 ISA Server 2004 发布非标准的 FTP 服务器时，不使用“FTP 筛选器”。如果是使用其他防火墙或者路由器的 NAT 方式，则直接做端口映射或者端口转发即可，如表 3-2 所示。

表 3-2 内网的 FTP 服务器

FTP 内网地址	FTP 服务端口	PASV 端口	PASV 地址	ISA 发布的端口
172.30.5.15	2115	2015	124.xx.xx.126	2115
172.30.5.16	2116	2016	124.xx.xx.126	2116
172.30.5.25	2125	2025	124.xx.xx.126	2125

其中，124.xx.xx.126 是 FTP 服务器所属网络中最外一级防火墙的外网地址（这个地址映射给了 FTP 服务器的防火墙的外网地址）。

在本节中，以内网地址为 172.30.5.15 的 FTP 服务器为例，将此 FTP 服务器使用 124.xx.xx.126 的 2115 端口发布（外网用户使用 ftp://124.xx.xx.126:2115 并用 PASV 方式即可以访问，可以使用 IE、CuteFTP、FlashGET 等多种客户端软件）。主要步骤如下：

第 1 步，在 172.30.5.16 的计算机上，打开 Serv-U 的控制台，设置 PASV 端口范围为 2006-2006，如图 3-52 所示。

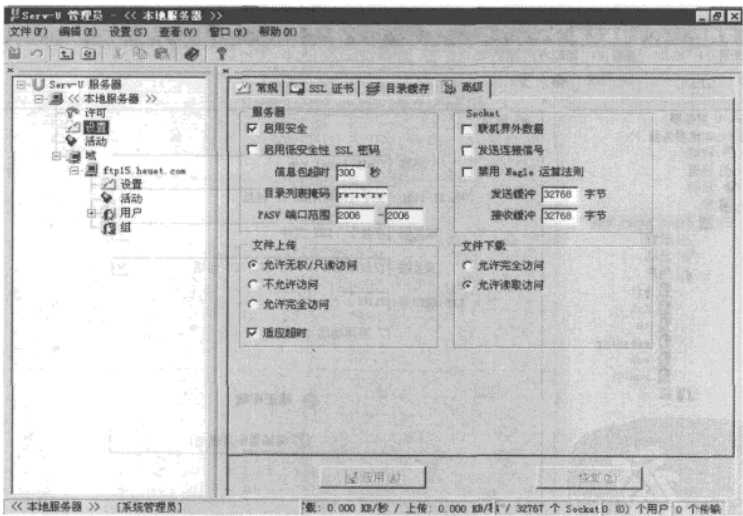


图 3-52 设置“PASV 端口范围”为 2006-2006

说明 在此只需要设置一个地址，可以允许最大量的用户访问，而不是一个端口只能连接一个 FTP 的客户端。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 2 步，选中“允许被动模式数据传输，使用 IP”复选框，并且设置 PASV 地址为防火墙映射的公网地址 124.xx.xx.126，如图 3-53 所示。

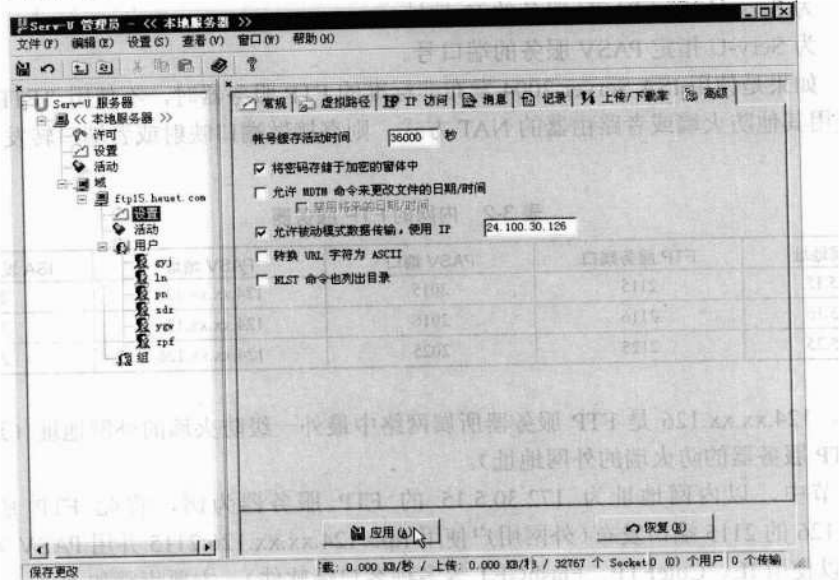


图 3-53 设置 PASV 地址

第 3 步，将 FTP 服务器的端口地址从默认的 21 修改为 2116，如图 3-54 所示。

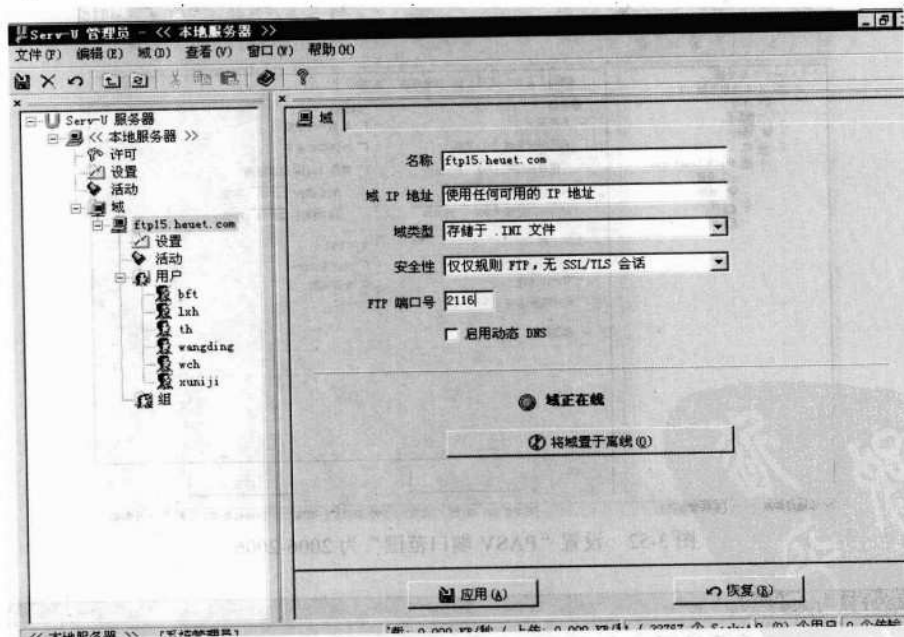


图 3-54 设置 FTP 端口号，默认为 21

第 4 步，然后重新启动 FTP 服务，如图 3-55 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

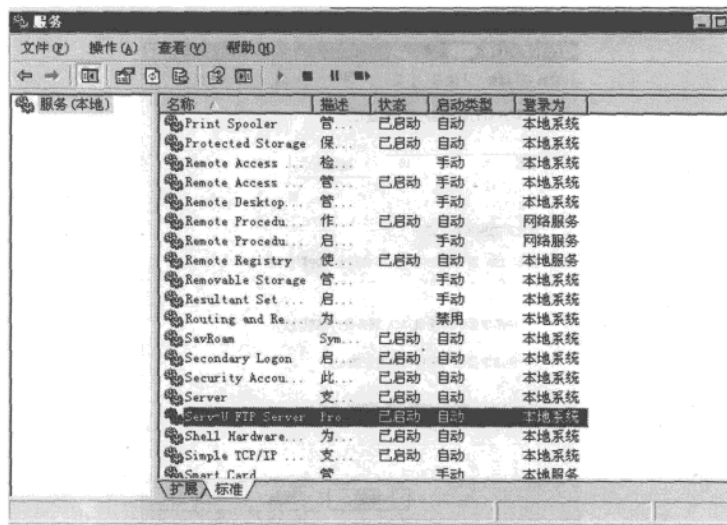


图 3-55 启动 FTP 服务

第 5 步，转到图 3-51 中的内网防火墙中进行设置，本例中使用 ISA Server 2004 (ISA Server 2006 与此相同)。如果是使用其他防火墙或者路由器的 NAT 功能，可以直接转发 TCP 的 2116 和 TCP 的 2006 到内网的 172.30.5.16 的 IP 地址上即可。下面以 ISA Server 为例说明。

在 ISA Server 2004 中，创建服务器发布规则，在“通信”中单击“新建”按钮，设置协议名称为“FTP:2116”，设置协议端口为 TCP 的 2006 和 TCP 的 2116（入站），如图 3-56 和图 3-57 所示。

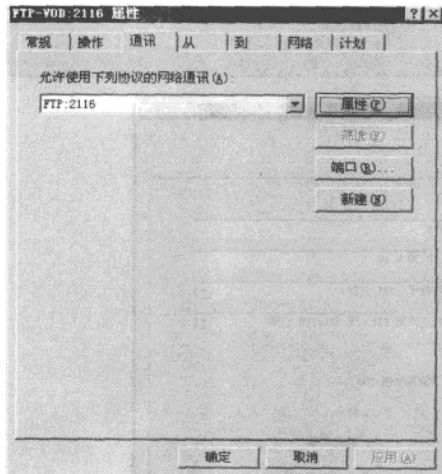


图 3-56 新建协议

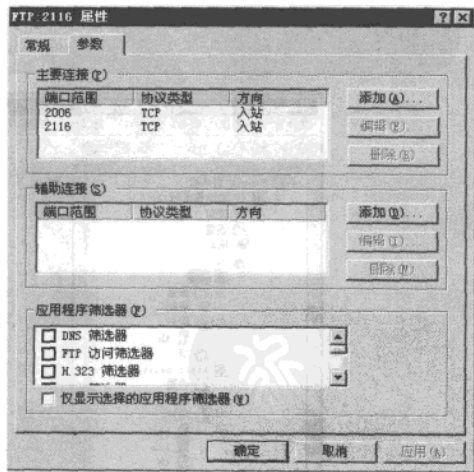


图 3-57 为内网 FTP 创建协议，指定 PASV 端口和 FTP 服务器发布端口

第 6 步，指定 FTP 服务器的内网地址“172.30.5.16”，并且选中“使请求显示为来自初始

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

客户端”单选按钮，如图 3-58 所示。

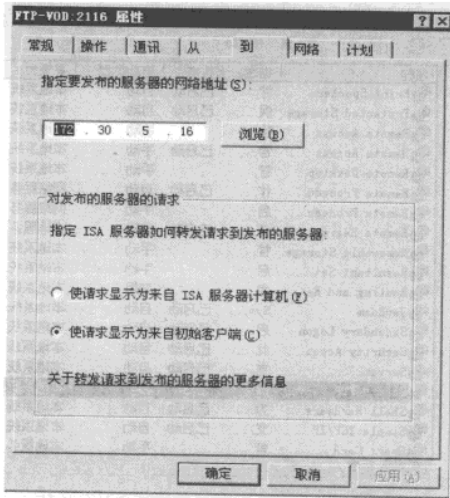


图 3-58 指定 FTP 的内网地址

创建服务器发布规则后，公网上的用户（包括公网上的内网用户）就可以使用 ftp://124.xx.xx.126:2116 访问以非标准端口发布的 FTP 服务器了。其他的内网服务器的发布，可以参照上面的步骤创建。

说·明

对于图 3-53 的网络，如果你想在内网中（IP 地址为 172.30.x.x 的网络）使用 21 端口访问 172.30.5.16 等 FTP 服务器，可以在 Serv-U 中，再创建端口为 21 的 FTP 服务器，因为 Serv-U 是支持多个不同端口的 FTP 服务器的，你只需要把相同的用户重建一下就可以了，如图 3-59 所示。

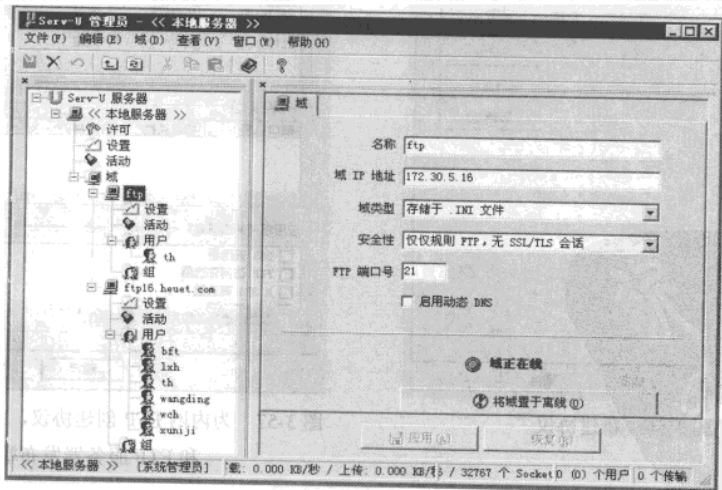


图 3-59 创建多个 FTP 服务器（端口不同）

3.2.5 用 Hotmail 空间组建自己的邮件系统的经验

许多公司、企业都申请了属于自己的域名，同时也创建了企业网站，可以在 Internet 上向顾客、合作伙伴，展示企业的产品并达到对外宣传、提供部分售后服务的目的。在公司对外的宣传彩页上和销售人员的名片上，也都印上了公司的网址。这一切表明公司的领导和员工，都对来自 Internet 方面的业务有了足够的重视。但是，在这些对外宣传中，有一个很关键的地址却被大家忽略了，那就是属于自己企业的邮件系统。

在许多员工的名片上，每个人使用的邮箱都是不同的，有的用 sohu 的，有的用网易的，或者新浪、yahoo 的，很少有人留的邮箱是公司（邮箱后缀与企业网站域名的后缀不同）的。造成这个问题的原因有许多，但一个最根本的原因就是，创建企业统一的邮件服务器，需要的投资是比较高的，并且维护费用也很高。而创建企业网站，只需要申请一个域名（每年大约几十元钱）、做一个网站，找个空间（每 MB 每年大约 1 元钱），这样，网站方面的费用可以省到忽略不计。但创建企业统一的邮件系统，则需要硬件、软件等多方面的投资（自己组建邮件服务器、自己接入 Internet 网络），或者使用第三方提供的邮件服务（例如一些提供网站空间的服务商），使这方面的费用居高不下。

那么，能不能创建属于自己的免费邮箱呢？例如，某单位申请的域名是 heuet.net，创建的网站是 www.heuet.net，能不能（免费）创建类似于 admin@heuet.net 的邮箱？微软的 Windows Live Domains 就提供了类似的服务。使用该服务，可以为一个域名创建最多 500 个邮箱，每个邮箱提供 200 MB 的空间，这可以满足一般的企业需要。并且，邮箱的数量以及每个邮箱的容量，还可以免费增加。下面以 heuet.net 域名为例，介绍这个产品的使用。

说
·
明

通常情况下，网上提供免费空间、免费邮箱很多，但提供的免费邮箱的域名后缀，都是厂商域名，例如，sohu 提供类似 xxx@sohu.com 的免费邮箱。

具体步骤如下：

第 1 步，登录 <http://domains.live.com>，进入 Windows Live 管理中心。在第一次使用时，请单击“开始”按钮，如图 3-60 所示。如果你已经登录过，再次使用时，请直接单击“登录”按钮。

第 2 步，在“提供你的域名”文本框中，输入你申请的域名。例如，在这里输入作者申请的域名 heuet.net，选中“为我的域设置 Windows Live Hotmail”单选按钮，然后单击“继续”按钮，如图 3-61 所示。

第 3 步，在“分配一个域管理员”页中，指定要管理 heuet.net 域 Windows Live 账户，你可以使用以前申请的 hotmail 或 msn 账户，也可以在你要创建的域中申请一个新的账户。推荐使用以前申请的 hotmail 或 msn 账户，在此选择“使用现有的 Windows Live ID 登录”单选按钮，然后单击“继续”按钮，如图 3-62 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

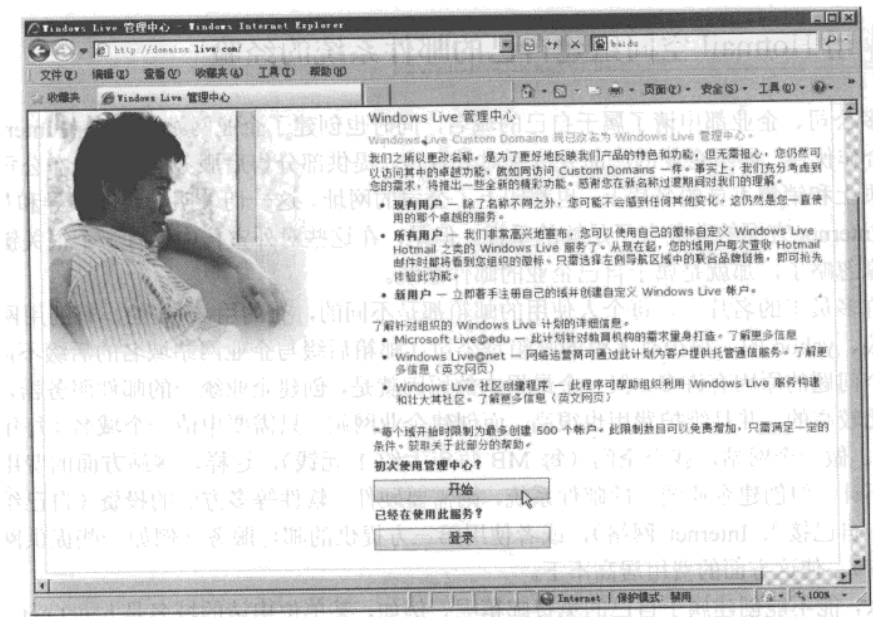


图 3-60 登录 Windows Live 管理中心

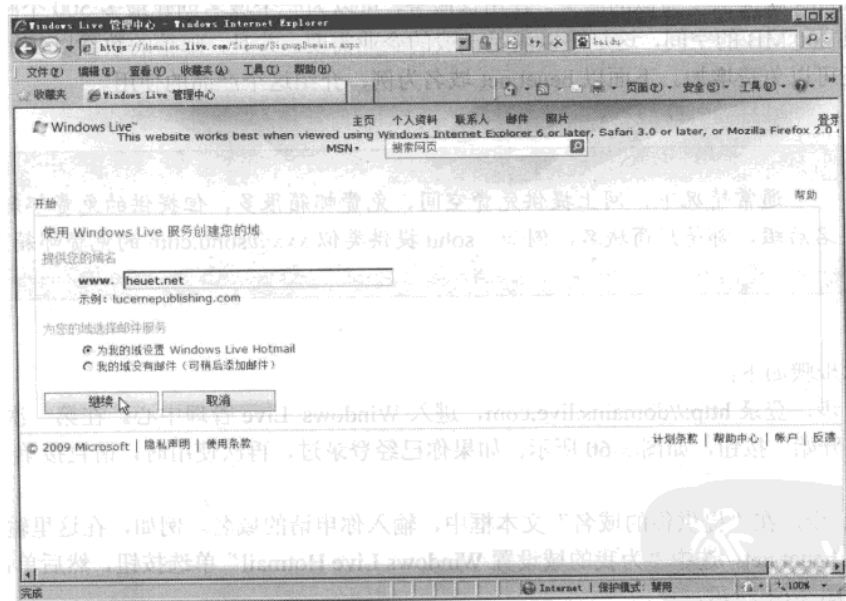


图 3-61 创建域

第 4 步，当前网页转到 Windows Live ID 登录页，请选择你的账户并登录，在此用一个 hotmail 账户登录，如图 3-63 所示。

第 5 步，登录之后，在“检查设置并接受协议”中，单击“我接受”按钮，如图 3-64 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

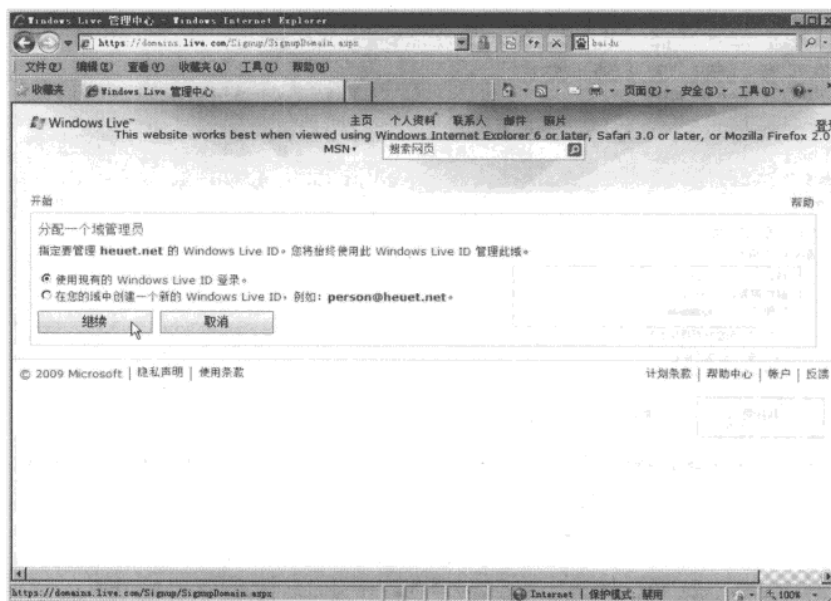


图 3-62 使用现有的 Windows Live ID 登录

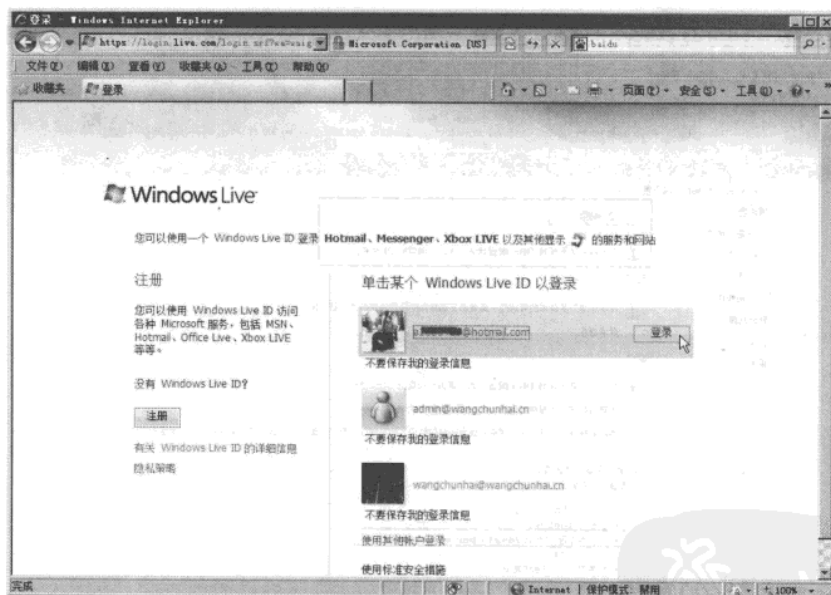


图 3-63 用 hotmail 账户登录

第 6 步，进入 Windows Live 管理中心，在网页中可以看到，你的 DNS 配置处于等待状态。此时，你需要配置 heuet.net 的 MX 记录，请记录下“MX 记录配置”中的“MX 服务器”后面的信息。在本例中，为 1959244214.pamx1.hotmail.com，如图 3-65 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

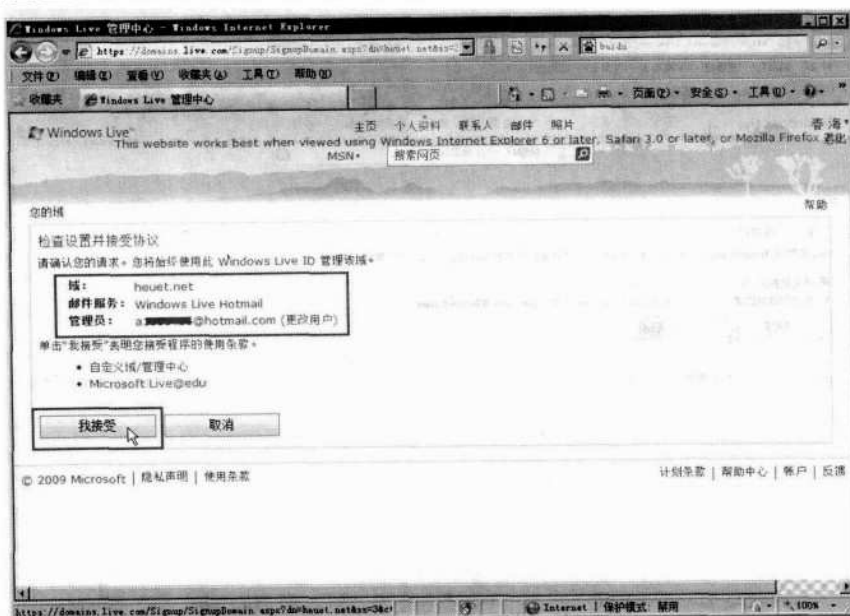


图 3-64 接受并管理



图 3-65 记下 MX 信息

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

第 7 步，切换到 heuet.net 的域名管理面板（通常在申请域名的时候，厂商会告诉你一个管理地址，用来管理 A 记录、MX 记录等，也可以看到域名的相关信息）。登录 heuet.net 的域名管理面板，在“域名自助解析”中，添加 MX 记录，需要注意，在添加 MX 记录时（有的域名管理面板是“邮件服务器名称”），输入图 3-65 中记录的地址，然后在“优先级别”中设置一个比较小的数值（在一个域有多个邮件服务器时，较小的数值代表较高的优先级），如图 3-66 所示。

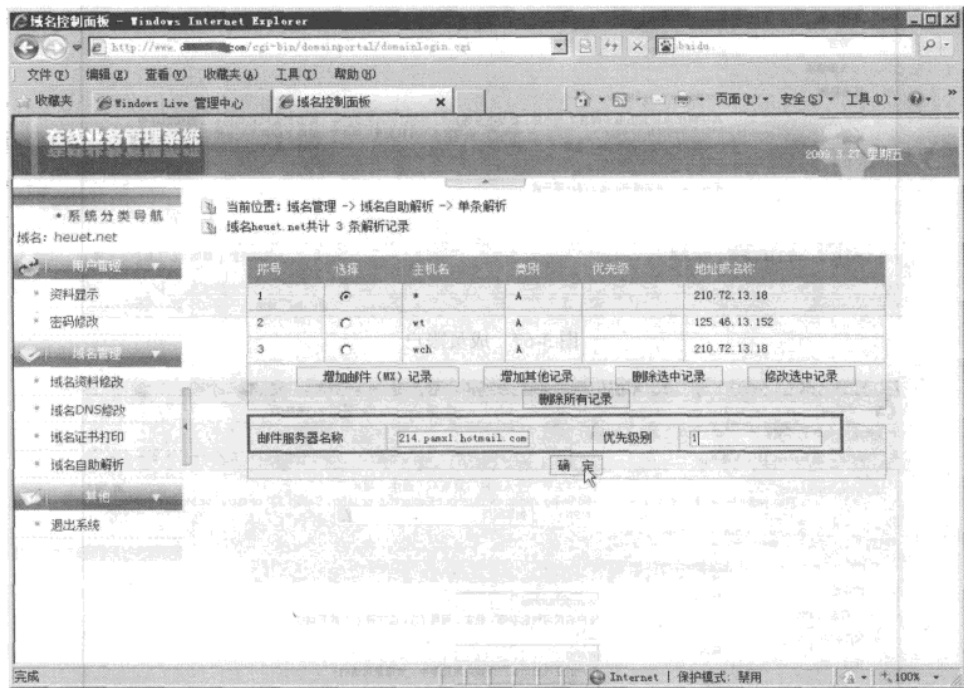


图 3-66 更新（或添加）MX 记录

说明 在添加 MX 记录后，通常需要 3 h 甚至更长的时间，DNS 信息才能同步到 Internet 中。

第 8 步，然后切换到图 3-65 界面，单击“刷新”按钮，请多等待一段时间，但最长不会超过 24 h。当 hotmail 邮件服务器检测到你的 MX 记录更新后，会进入“成员账户”页，此时，单击“添加”按钮，就可以添加以@heuet.net 为后缀的邮箱了，如图 3-67 所示。

第 9 步，添加账户页面，如图 3-68 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

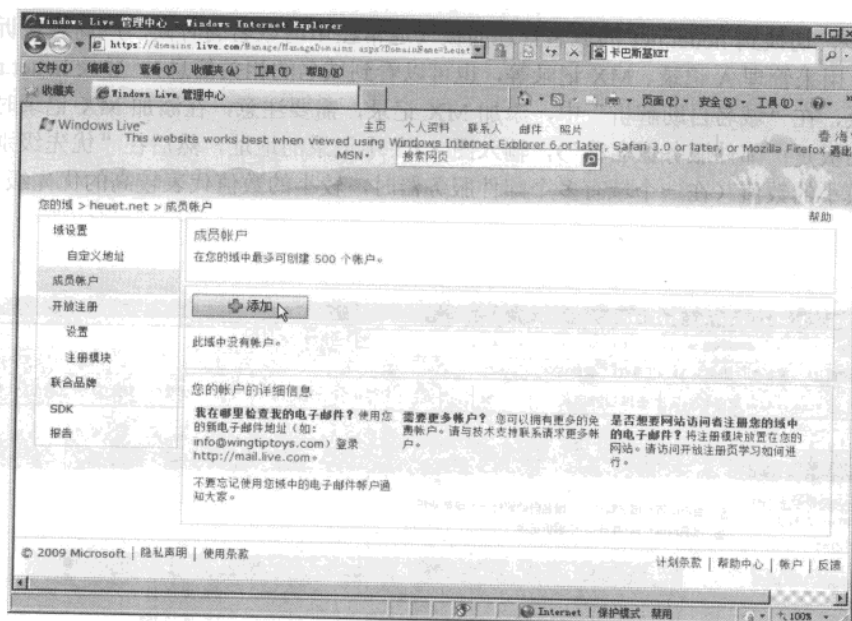


图 3-67 成员账户

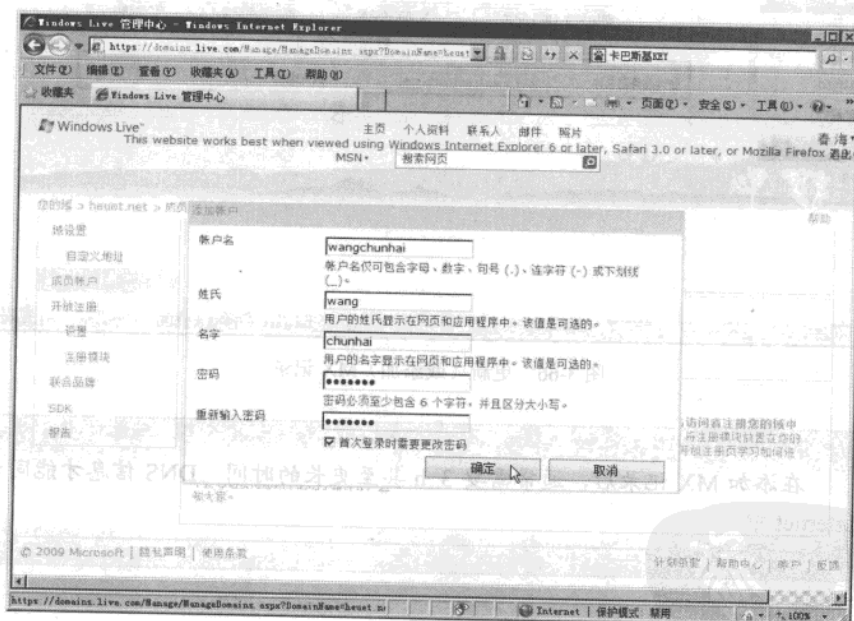


图 3-68 添加账户

说
·
明

在一个域中，可以添加 500 个账户。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

第 10 步，选择“开放注册”，然后选择“设置”，在右侧单击“启用开放注册”按钮，如图 3-69 所示。

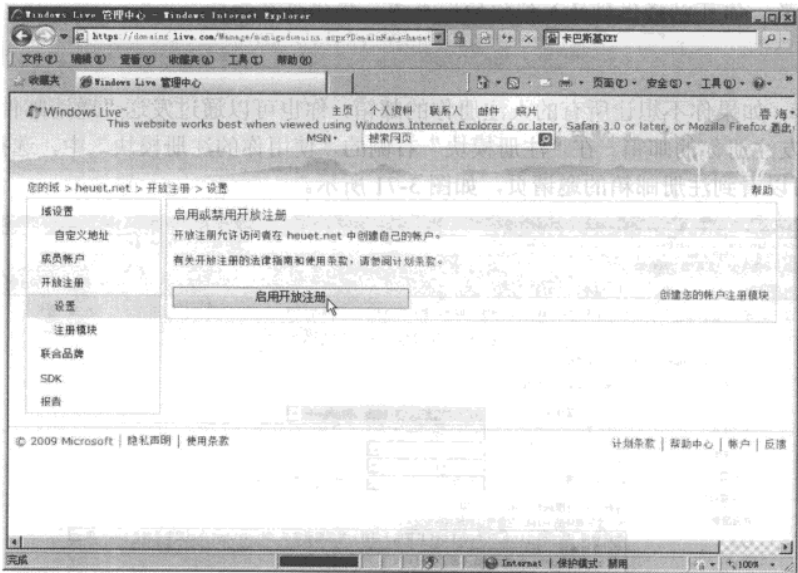


图 3-69 启用开放注册

第 11 步，选择“注册模块”选项，在右侧可以查看网页中的“开放注册”代码，如图 3-70 所示。

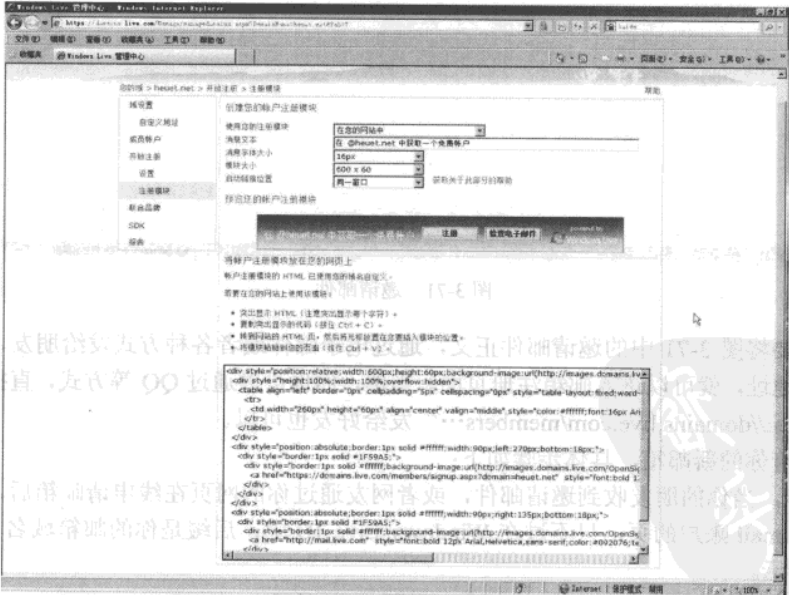


图 3-70 在网页中的“开放注册”代码

网管天下 网管经验谈

注意 在图 3-70 所示“预览你的账户注册模块”中，可以看到开放注册的按钮及效果。你可以将代码嵌入到你的网页中，提供这个功能。

第 12 步，如果你不想让所有的人注册你的邮箱，你也可以通过发送“邀请邮件”的功能，让指定的朋友注册你的邮箱。在“注册模块”右侧的“使用你的注册模块”中，选择“在邀请邮件中”，可以看到注册邮箱的邀请页，如图 3-71 所示。

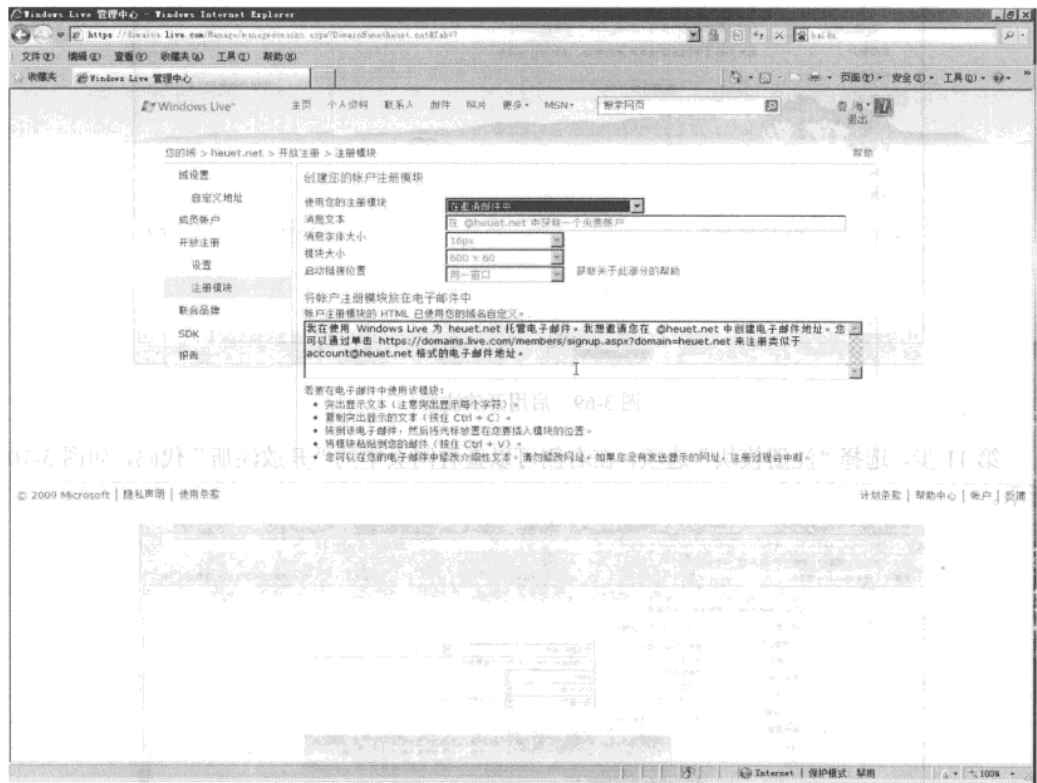


图 3-71 邀请邮件

你只需要将图 3-71 中的邀请邮件正文，通过电子邮件或者各种方式发给朋友，对方单击其中的链接地址，就可以进入邮箱注册页面。当然，你也可以通过 QQ 等方式，直接将邮件正文中的“https://domains.live.com/members...”发给好友也可以。

如何申请你的新邮箱，具体步骤如下：

第 1 步，当你的朋友收到邀请邮件，或者网友通过你的网页在线申请邮箱后，会进入类似于申请 hotmail 账户的页，只不过在 Windows Live ID 中，后缀是你的邮箱域名 heuet.net，如图 3-72 所示。

第 2 步，申请完成后，就进入新邮箱，如图 3-73 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

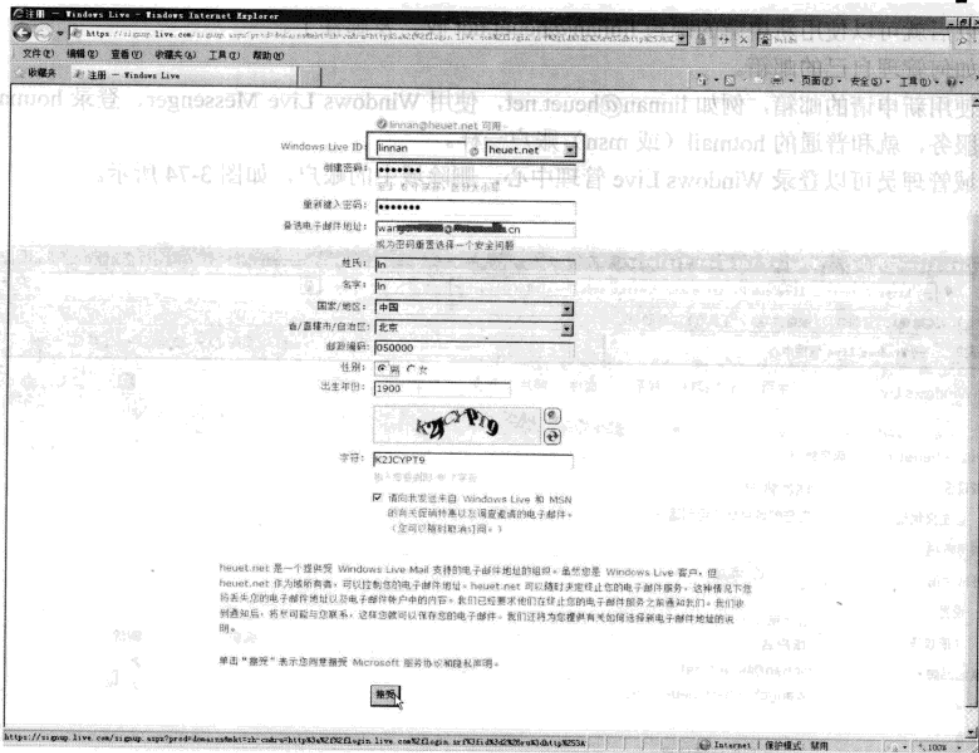


图 3-72 邮箱注册页

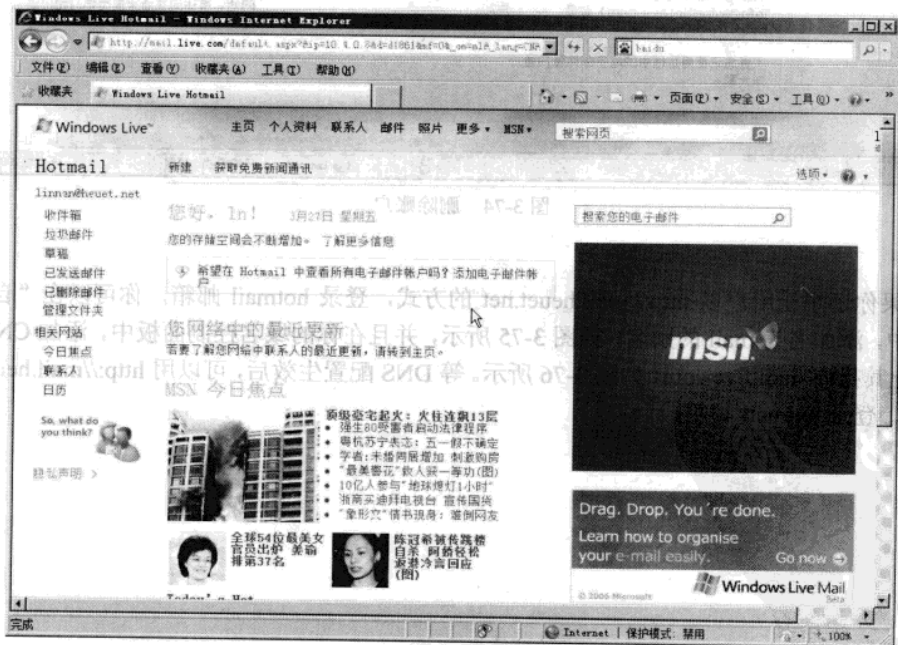


图 3-73 进入 hotmail 邮箱

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

以后就可以使用新申请的邮箱 `linnan@heuet.net` 收、发邮件了。

如何管理自己的邮箱。

使用新申请的邮箱，例如 `linnan@heuet.net`，使用 Windows Live Messenger、登录 hotmail 邮箱服务，就和普通的 hotmail（或 msn）账户一样。

域管理员可以登录 Windows Live 管理中心，删除域中的账户，如图 3-74 所示。



图 3-74 删除账户

如果你还想让用户以 `http://mail.heuet.net` 的方式，登录 hotmail 邮箱，你可以在“自定义地址”中，添加名为 mail 的别名，如图 3-75 所示，并且在你的域名控制面板中，添加 CNAME 记录，让其指向 `mail.live.com`，如图 3-76 所示。等 DNS 配置生效后，可以用 `http://mail.heuet.net` 的方式，登录 hotmail 邮箱。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

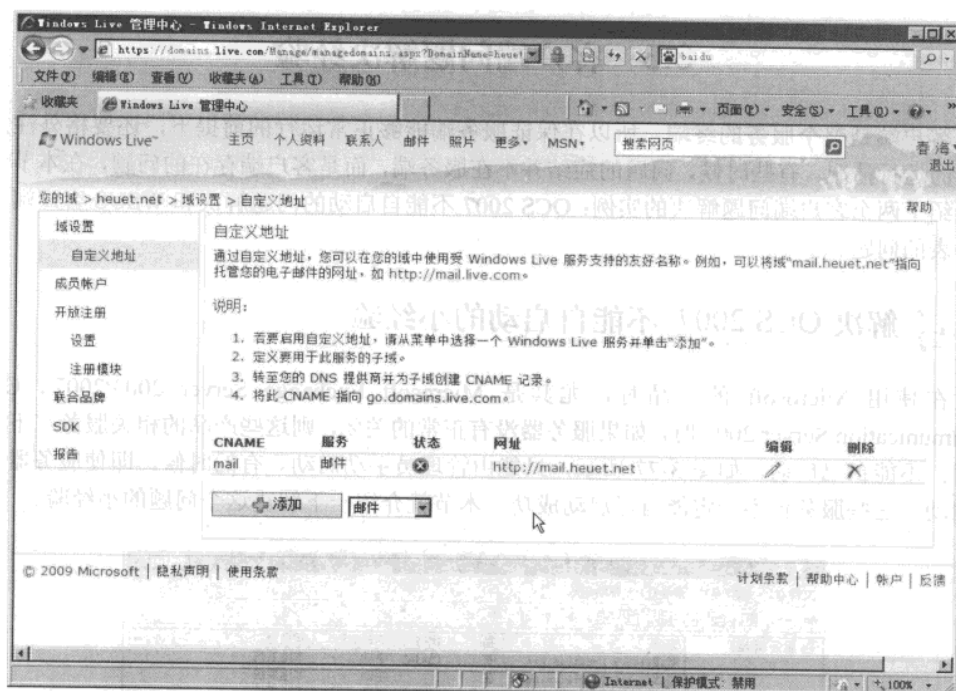


图 3-75 添加别名

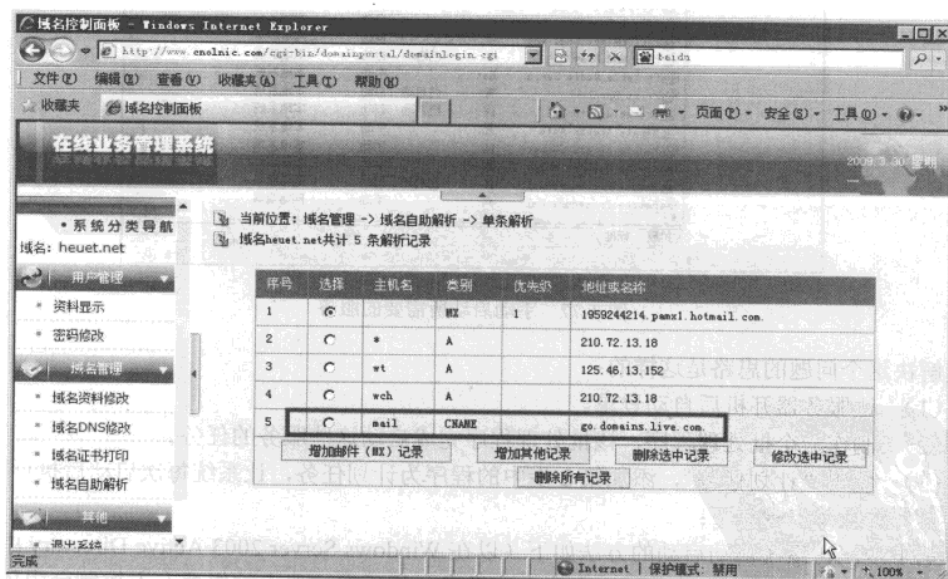


图 3-76 添加 CNAME 记录指向 hotmail

3.3 客户端问题解决经验

客户端是整个服务的终端，所以在保证服务端能够正常运行的前提下，还要格外注意客户端的运行情况。有些时候，问题的症结并不在服务端，而是客户端存在的问题，在本节中我们介绍了两个客户端问题解决的实例：OCS 2007 不能自启动的问题解决和 WSUS 客户端导入注册表的问题。

3.3.1 解决 OCS 2007 不能自启动的小经验

在使用 Microsoft 的产品时，尤其是 Microsoft Exchange Server 2003/2007、Office Communication Server 2007 时，如果服务器没有正常的关闭，则这些产品的相关服务在下次启动时，不能自己启动，如图 3-77 所示，只能由管理员手动启动。有的时候，即使服务器是正常启动，这些服务也不一定能自己启动成功。本节就介绍一下解决这个小经验。

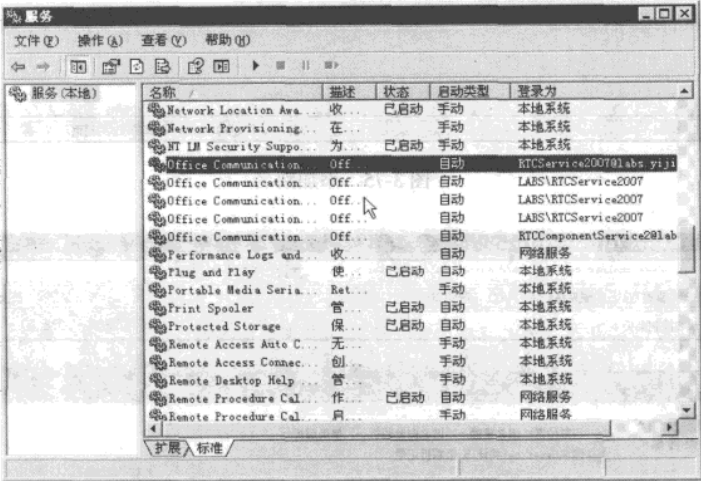


图 3-77 手动启动所需要的服务

- 解决这个问题的思路是这样的：
- (1) 让服务器开机后自动登录。
 - (2) 制作一个批处理程序，该批处理程序完成启动这些服务的任务。
 - (3) 使用“计划任务”，添加第 2 步中的程序为计划任务，让系统每次启动后执行。
- 具体的操作步骤如下：

第 1 步，让系统自动启动的方法如下（以在 Windows Server 2003 Active Directory 中的登录方法为例）：运行“regedit”打开注册表编辑器，然后在注册表编辑器左方控制台中依次单击展开“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon”，再选择“新建-字符串值”，在数值名称中输入“AutoAdminLogon”，设置键值为“1”，如图 3-78 所示，实现自动登录的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

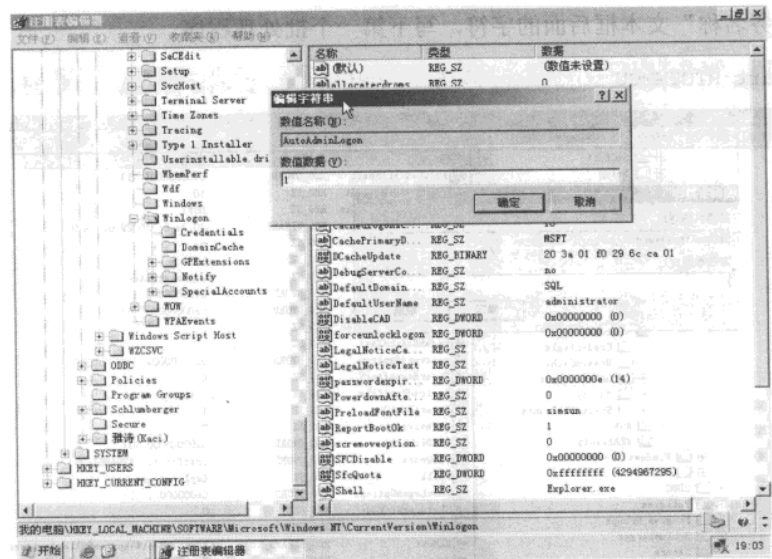


图 3-78 新建 “AutoAdminLogon”

第 2 步，检查是否有 “DefaultUserName” 的字符串值（msft\administrator），检查 “DefaultDomainName” 值是否是域的 NetBIOS 名称，如图 3-79 所示，如果这两项都是上次登录的用户名和域名就不用再次编辑。



图 3-79 核对登录用户及域名

第 3 步，创建一个名为 “Defaultpassword” 的字符串值，并编辑字符串为你准备用于自动登录的用户账户密码，如图 3-80 所示。编辑完并检查无误后，关闭注册表编辑器并重新启动计算机即可自动登录。

第 4 步，创建启动批处理程序。双击图 3-77 中需要启动的服务，如图 3-81 所示。记下图

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

3-81 中“服务名称”文本框后面的字符，写下第一个批处理程序。

```
net start RTCIMMCU
```

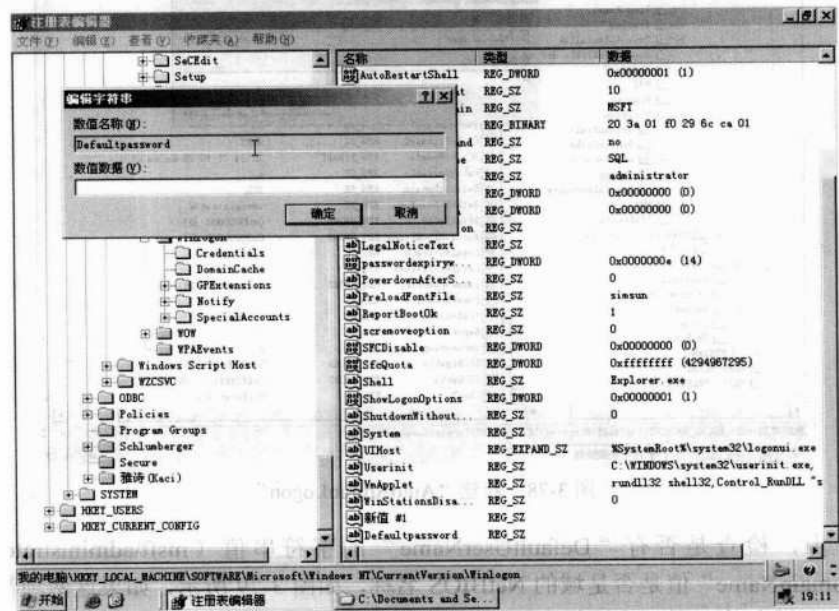


图 3-80 创建“Defaultpassword”



图 3-81 创建第一个批处理程序

第 5 步，依次记下需要启动的每个服务，对于 OCS2007 来说有 5 个，分别是：

```
net start RTCIMMCU
net start RTCDATAMCU
net start RTCACPMCU
net start RtcSrv
net start RTCAVMCU
```


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

之后将该批处理程序保存在桌面或者其他一个文件夹中。Exchange 2007/2003 的启动和 ocs2007 一样不在做过多介绍。

第 6 步，在“附件”→“系统工具”中选择“计划任务”，添加计划任务，如图 3-82 所示。进入“任务计划向导”页，输入任务名称，并选择“登录时”执行这个任务，然后单击“下一步”按钮。

第 7 步，在图 3-83 中输入自启动时，进入系统的用户名及密码，实现开机后自动登录的功能，单击“下一步”按钮。

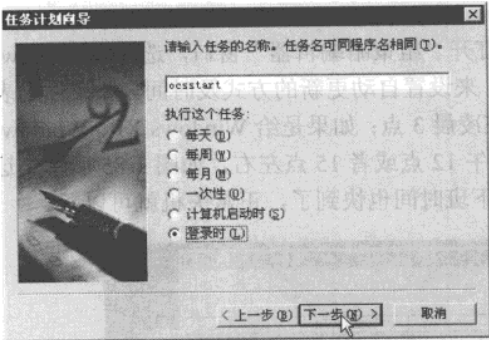


图 3-82 创建任务计划

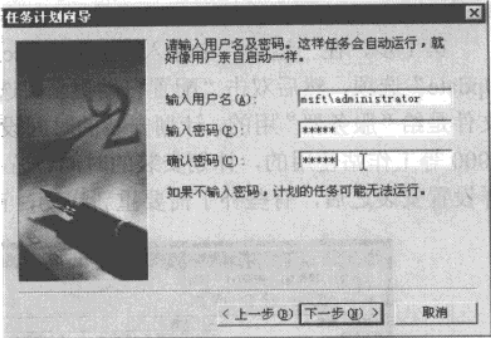


图 3-83 输入启动用户名及密码

第 8 步，创建计划任务完成后，打开“任务”选项卡，选中“仅在登录后运行”复选框，如图 3-84 所示。单击“确定”按钮，完成自启动的设置功能。

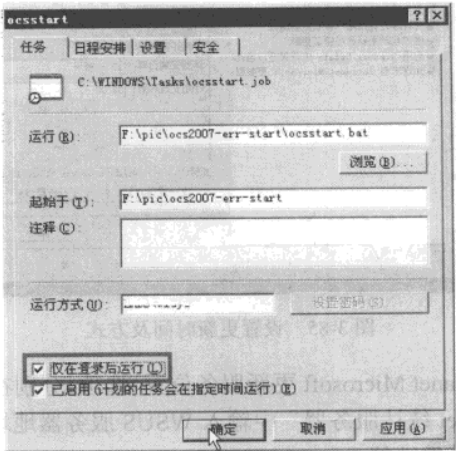


图 3-84 设置运行环境

经过上面的操作后，即使 Exchange 或 OCS 非正常关机，在服务器重新启动后，也能自动启动所需要的服务。

3.3.2 关于使用 WSUS 时客户端导入注册表文件的解决方法

在使用 WSUS 服务器时，需要在客户端上使用 gpedit.msc 配置 update 组件，对于管理员

网管天下 网管经验谈

来说，这是一个简单的问题，但对于普通用户来说，相对比较复杂。另外，有一些工作站是 Windows XP Home 版本，这个版本是没有 gpedit.msc 的。为了解决这两个问题，一般来说，管理员都是从网上找 WSUS 客户端的注册表导入文件，但找到的注册表导入文件可能不适合自己单位使用，例如：有的注册表导入文件中，是需要“手动”安装补丁的；有的虽然是“自动”安装补丁，但安装补丁的“时间”不对。本节就介绍一下如何根据自己的需要定制自己的 WSUS 客户端的注册表导入文件。思路是在一台 Windows XP Professional 的计算机上，根据单位的实际情况进行配置，然后导出注册表文件供本单位自己使用就可以了，具体的操作步骤如下。

第 1 步，在“运行”中输入“gpedit.msc”，打开“组策略编辑器”窗口，选择“Windows Update”选项，然后双击“配置自动更新”选项。来设置自动更新的方式及时间。如果注册表文件是给“服务器”用的，计划安装的时间设置在凌晨 3 点；如果是给 Windows XP、Windows 2000 等工作站使用的，计划安装的时间设置在中午 12 点或者 15 点左右，如图 3-85 所示。这样设置安装之后，有些补丁需要重新启动，正好下班时间也快到了，正常关机就可以了。

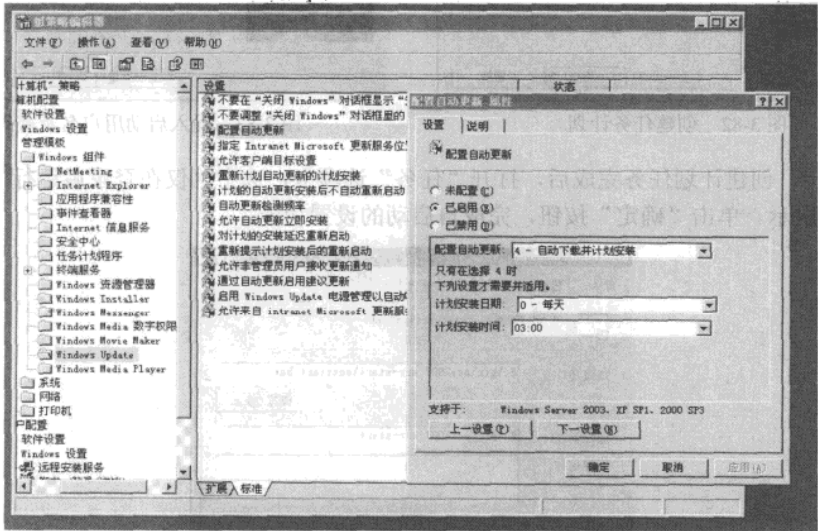


图 3-85 设置更新时间及方式

第 2 步，双击“指定 Intranet Microsoft 更新服务位置”选项，分别在“为检测更新设置 Intranet 更新服务”和“设置 Intranet 统计服务器”中输入 WSUS 服务器地址及端口，如图 3-86 所示，实现设置升级服务器的地址的功能。

第 3 步，双击“允许自动更新立即安装”选项，在其属性对话框中启用该服务，如图 3-87 所示，实现允许自动更新立即安装的功能。

第 4 步，双击“允许非管理员用户接收更新通知”选项，在其属性对话框中启用该项，如图 3-88 所示，实现允许非管理员用户接收更新通知的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

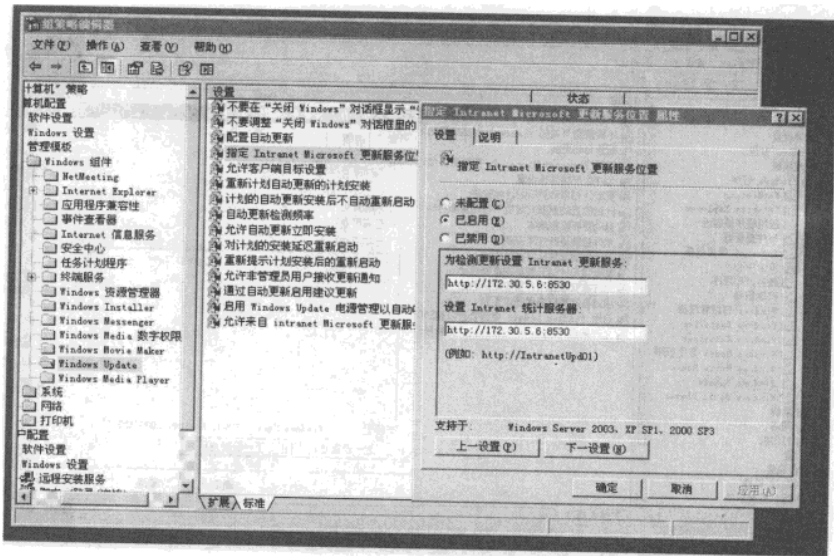


图 3-86 设置服务器地址及端口

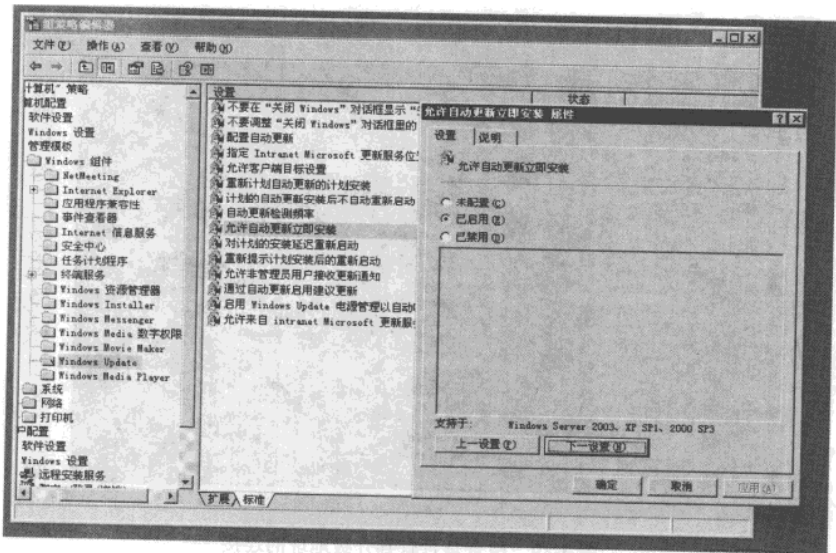


图 3-87 启用“允许自动更新立即安装”

第 5 步，设置完成后，进入命令提示符，执行“wuauclt /detectnow”和“wuauclt /detectnow”，然后执行“netstat -an”，检查是否有到升级地址的连接。如果有，表示设置正确，并且 WSUS 服务器工作正常，如图 3-89 和图 3-90 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

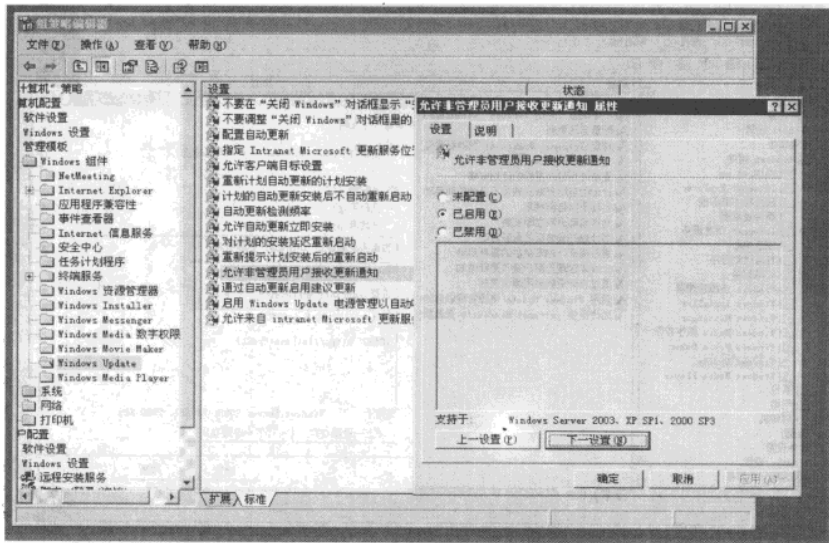


图 3-88 允许非管理员用户接收更新通知

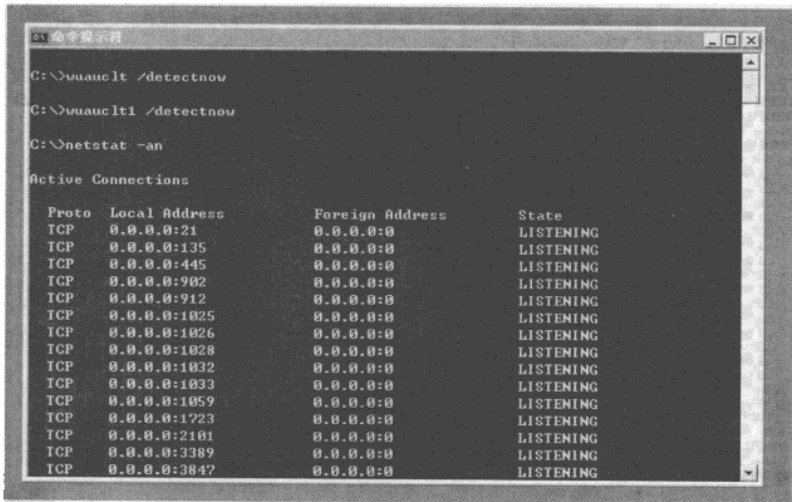


图 3-89 检查是否有到升级地址的连接

第 6 步，在“运行”中输入“regedit”，打开“注册表编辑器”窗口，依次选择“HKEY_LOCAL_MACHINE”、“SOFTWARE”、“Policies”、“Microsoft”、“Windows”和“WindowsUpdate”，并右击“WindowsUpdate”，在弹出的快捷菜单中选择“导出”命令，如图 3-91 所示。实现“HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate”键值导出的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

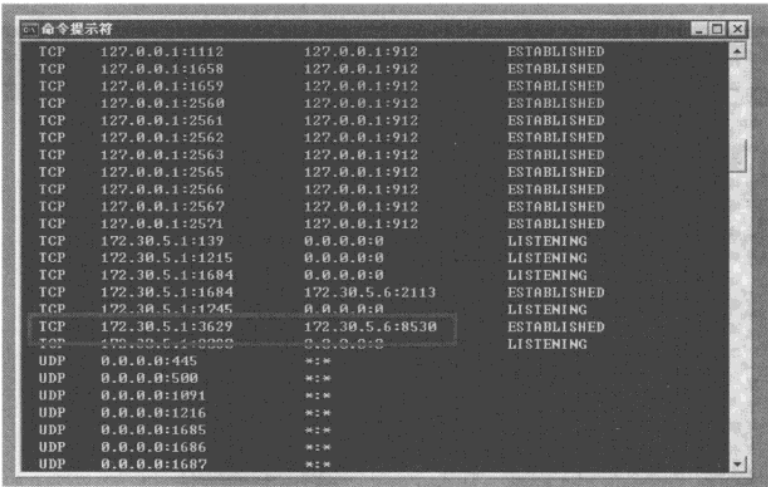


图 3-90 接收到升级地址的连接

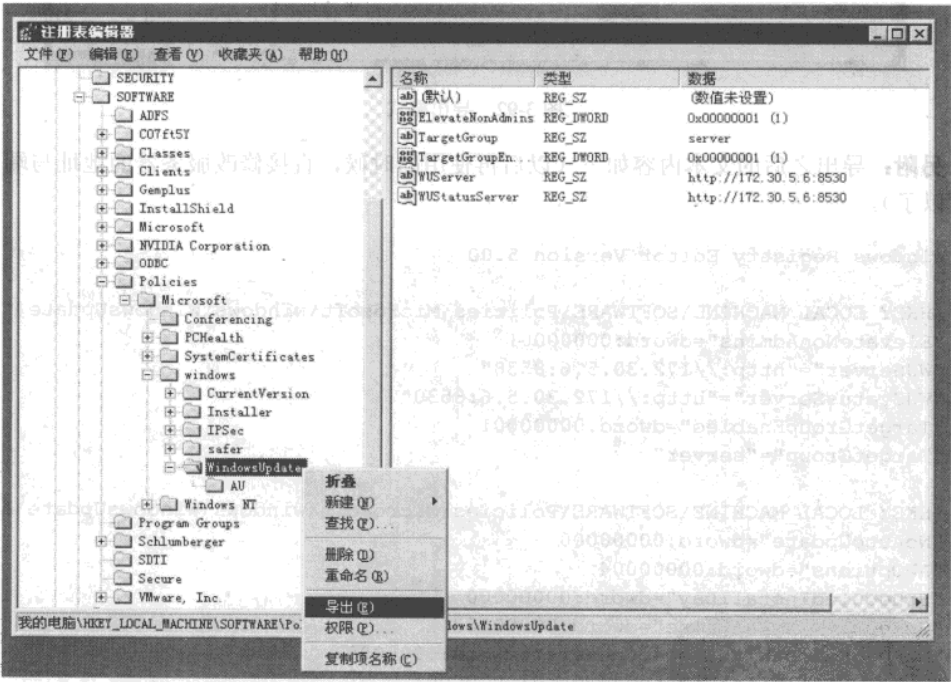


图 3-91 导出注册表信息

第 7 步，导出的时候，以“wsus_WSUS-IP-port”格式命名，如图 3-92 所示，实现容易区分的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

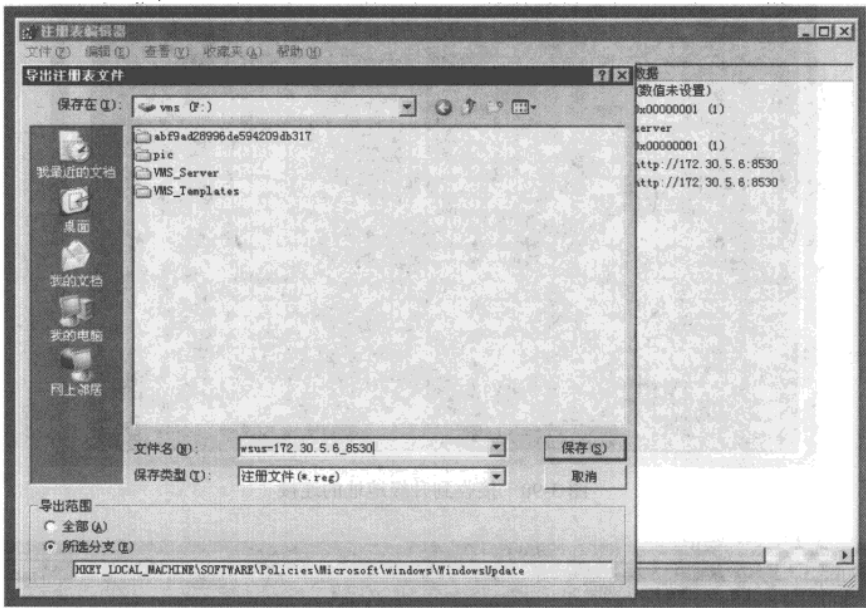


图 3-92 导出格式

另附：导出之后的文本内容如下（以后再使用的时候，直接修改服务器的地址与端口号就可以了）。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\WindowsUpdate]
"ElevateNonAdmins"=dword:00000001
"WUServer"="http://172.30.5.6:8530"
"WUStatusServer"="http://172.30.5.6:8530"
"TargetGroupEnabled"=dword:00000001
"TargetGroup"="server"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\WindowsUpdate\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"AutoInstallMinorUpdates"=dword:00000001
"NoAUAsDefaultShutdownOption"=dword:00000001
"UseWUServer"=dword:00000001
"RescheduleWaitTimeEnabled"=dword:00000001
"RescheduleWaitTime"=dword:00000001
"DetectionFrequencyEnabled"=dword:00000001
"DetectionFrequency"=dword:00000016
"RebootWarningTimeoutEnabled"=dword:00000001
"RebootWarningTimeout"=dword:00000005
```



```
"RebootRelaunchTimeoutEnabled"=dword:00000001  
"RebootRelaunchTimeout"=dword:0000000a
```

3.4 增强服务器功能的经验

一台物理的服务器所实现的功能毕竟有限，但是为了实现更多的功能去购买另外的服务器未免有点破费。为了使现有的服务器资源充分利用起来，我们就必须用各种方法增强服务器的功能。本节介绍了 App-V 和 RMS 等服务器的使用经验，来更好地提升服务器的功能。

3.4.1 App-V 使用经验

Microsoft Application Virtualization 4.5 是 Microsoft 虚拟化产品中“应用程序虚拟化”部分的组成部分。本节将介绍 Microsoft Application Virtualization 4.5（以下简称 App-V）的使用经验与注意事项。

1. App-V 服务器端安装注意事项

App-V 整个系统由三部分组成：服务器端、客户端、应用程序序列化端。其中“应用程序序列化端”是将需要虚拟化的软件，例如 Microsoft Office、WPS 等，转化成适合虚拟化应用的程序。App-V 整个系统需要 Active Directory 的支持，其中服务器端、客户端都需要加入到 Active Directory，应用程序序列化端虽然不需要加入到 Active Directory，但是也建议将其加入到 Active Directory。App-V 服务器端安装程序名称为“Microsoft System Center Application Virtualization Management Server 4.5”，需要安装在 Windows Server 2003 或 Windows Server 2008 系统上，需要 IIS 的支持。

说
明

如果所使用的网络中，有多个 VLAN，为了使用 NetBIOS 名称解析 App-V 服务器端的名称，需要在网络中配置 WINS 服务器。否则，与 App-V 服务器不在同一 VLAN 中其他客户端，不能访问 App-V 服务器。一般情况下，不要同时安装“Microsoft System Center Application Virtualization Streaming Server 4.5”。根据我的测试，如果安装这个软件，则客户端与服务器连接时需要使用 RTSPS 的连接。

App-V 系统的流程如下：

- （1）在 Windows Server 2003（或 2008）系统上，安装 App-V 服务器端，申请证书，创建共享文件夹。
- （2）在一台 Windows XP（或 Vista）系统上，安装 App-V 序列化端，并且将一个分区盘符修改为 Q，然后使用序列化工具、安装并封装要在 App-V 系统中使用的软件，例如 Office、下载快车、暴风影音等。最后，将序列化的软件上传到 App-V 服务器端。
- （3）切换到 App-V 服务器端，使用 App-V 管理器，导入第（2）步中封装的程序。
- （4）在 App-V 客户端，测试（使用）App-V 序列化后的软件。
- （5）在使用一段时间后，如果有的软件需要升级，例如 Office 2003 要升级 SP3，则使用

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

App-V 序列化工具，导入原来的程序，升级 Office。
检查服务器的计算机名称。

在管理 App-V 服务器之前，需要申请“计算机证书”。在申请证书的时候，申请的证书名称要与计算机名称相同，例如，在本例中，计算机名称为 app-v，则申请证书的名称也要为 app-v。为了简化，可以直接使用“Internet 信息服务管理器”来申请证书，如图 3-93 所示。

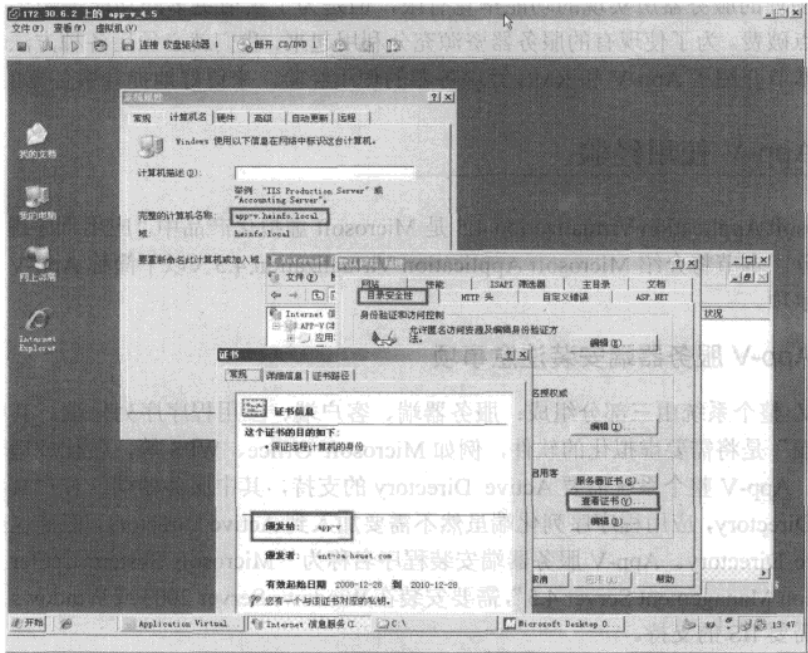


图 3-93 申请的证书与计算机的 NetBIOS 名称相同

App-V Server 也需要 SQL Server 的支持，其中 SQL Server 可以与 App-V Server 安装在同一台服务器上，也可以使用网络中的任意一台 SQL Server。在安装的过程中，如果 SQL Server 服务器没有安装在本机，安装程序会自动搜索当前网段是否有 SQL Server：如果有，会自动列出可用的 SQL Server 服务器；如果当前网段没有 SQL Server，而要使用其他 VLAN 中的 SQL Server 服务器，可以指定 SQL Server 服务器的计算机名称。

安装完成后，需要将“C:\Program Files\Microsoft System Center App Virt Management Server\App Virt Management Server\content”文件夹设置成共享，并设置共享权限：让普通用户只读、让管理员完全控制，如图 3-94 所示。共享名称可以随意设置，这一点没有特殊的要求。一般情况下，使用默认的名称“content”即可。

2. 应用程序序列化端注意事项

应用程序序列化端（安装程序为“Microsoft Application Virtualization Sequencer 4.5”）需要安装在 Windows XP 或 Windows Vista 的计算机上。最好找一台“全新”系统的计算机（或虚拟机），在该计算机上，只安装操作系统、驱动程序，不要安装其他软件。

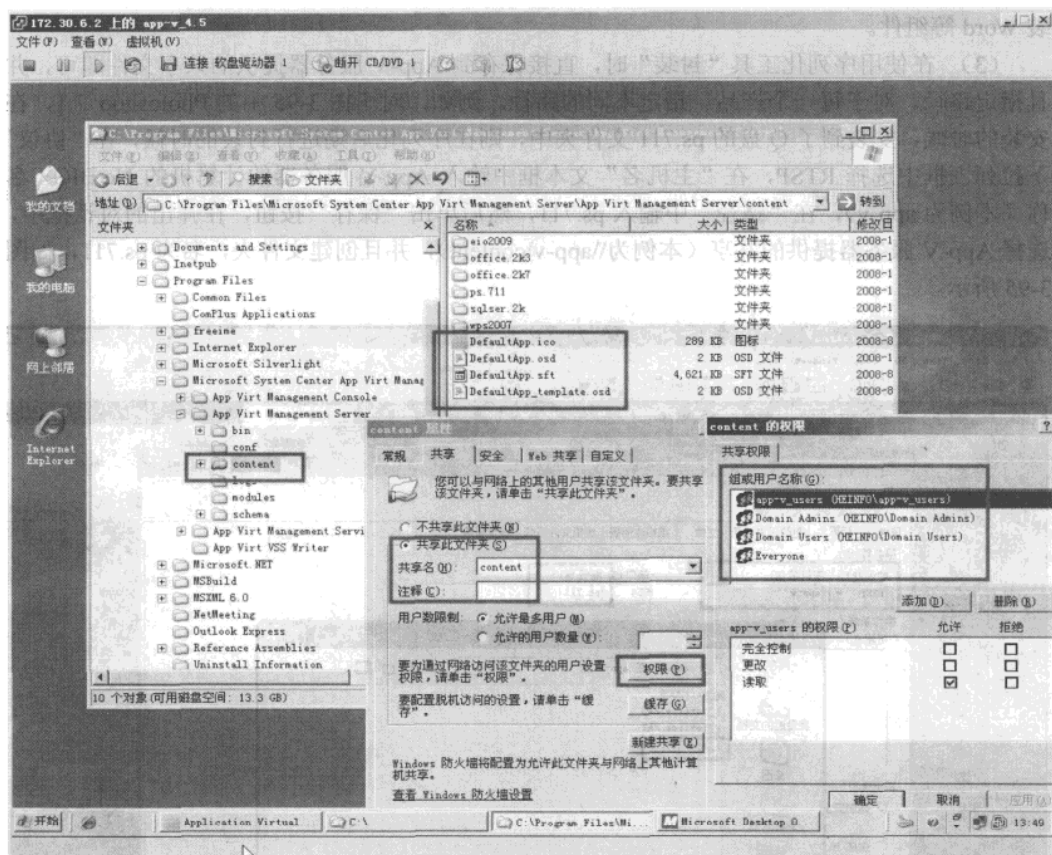


图 3-94 创建共享

应用程序序列化端的计算机，需要至少有两个分区，其中：一个分区是“系统”分区，安装操作系统与应用程序序列化端软件（即 App-V Sequencer 4.5）；另一个分区，需要使用“磁盘管理器”，将盘符修改为 Q，在序列化软件的过程中，所有的软件都要安装在该分区。

3. 关于使用“序列化工具”时的注意事项

在使用序列化工具时，为了简化管理、方便以后增加或删除序列化后的软件，需要注意以下问题：

（1）将每个软件安装在一个单独的文件夹中，并且文件夹的长度符合 8.3 的规则（DOS 下命名文件名的一种规格：主文件名是小于等于 8 个英文字符，扩展名为特定的某 3 个英文字符，他们之间必须用“.”连接起来，构成一个完整的文件名。），例如，可以将 Office 2007 安装在 Q 盘的 Office.2k7 文件夹中，将 Office 2003 安装在 Q 盘的 Office.2k3 文件夹中，将 WPS 2007 安装在 wps2007 文件夹中。

（2）安装的时候，要选择“自定义安装”，选择安装路径（Q 盘），并且选择好要使用的产品。例如，对于 Office 企业版来说，可以选择安装 Word、Excel、PowerPoint 等。对于每一个产品，最好选择“完全安装”，例如在安装 Office 2007 的时候，对于 Word 来说，要完全安

装 Word 等组件。

(3) 在使用序列化工具“封装”时，直接保存到 App-V 服务器提供的共享文件即可，并且指定路径。对于每一个产品，指定不同的路径。例如，对于图 3-95 中的 Photoshop 7.1，在安装的时候，安装到了 Q 盘的 ps.711 文件夹中，则在序列化后期进行封装的时候，在“协议”下拉列表框中选择 RTSP，在“主机名”文本框中输入 App-V 服务器的计算机的 NetBIOS 名称（本例为 app-v），在“路径”中输入 ps.711，然后单击“保存”按钮，在弹出的对话框中，选择 App-V 服务器提供的共享（本例为 \\app-v\\content），并且创建文件夹，名为 ps.711，如图 3-95 所示。

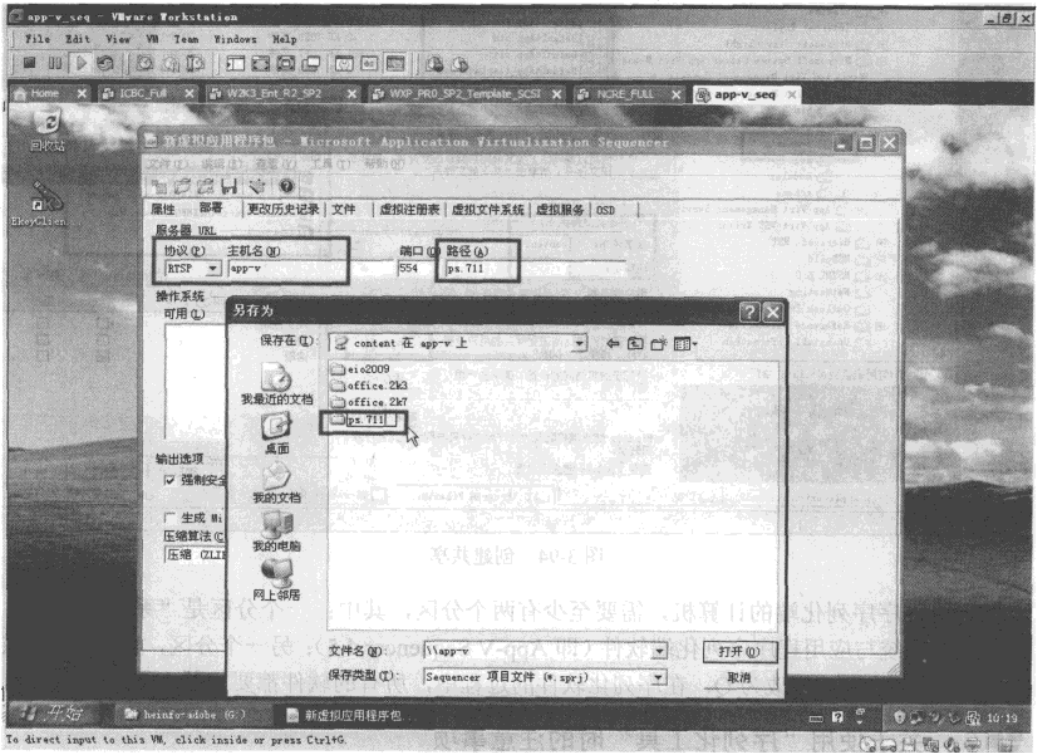


图 3-95 指定路径

然后，在“文件名”处输入保存后的包名，例如 photoshop 7.1。

4. 对序列化后的软件包进行升级时的注意事项

在这里我们以将 Office 2003 更新到 SP3 为例，具体操作步骤如下：

第 1 步，在序列化工具中，打开“文件”菜单，选择“打开进行包升级”命令，如图 3-96 所示。

第 2 步，浏览 \\app-v\\content 文件夹，打开 Office.2k3 下的 Office2003.sprj，如图 3-97 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

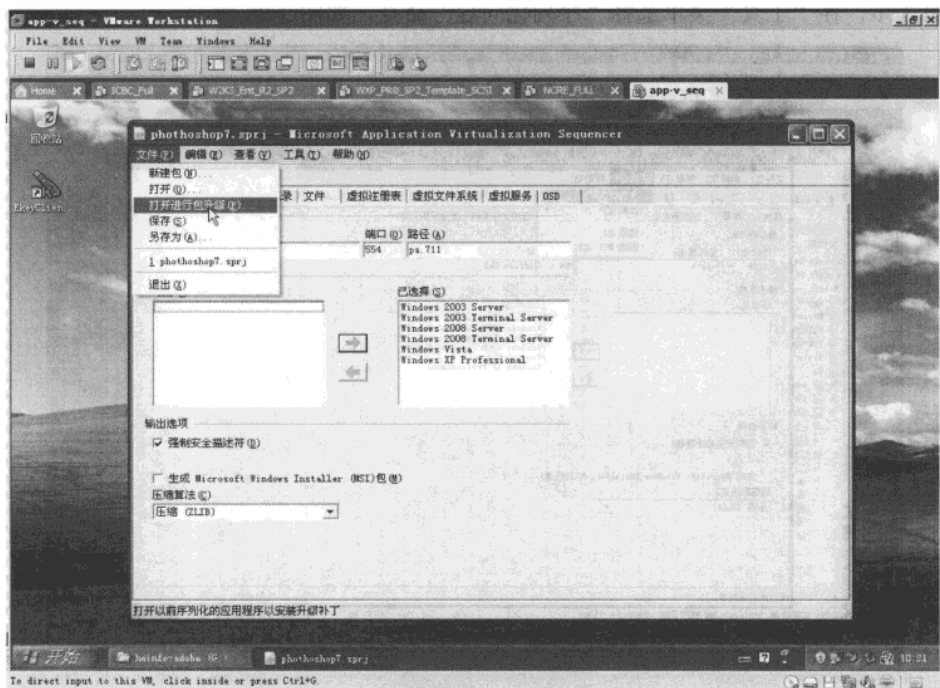


图 3-96 打开包进行升级

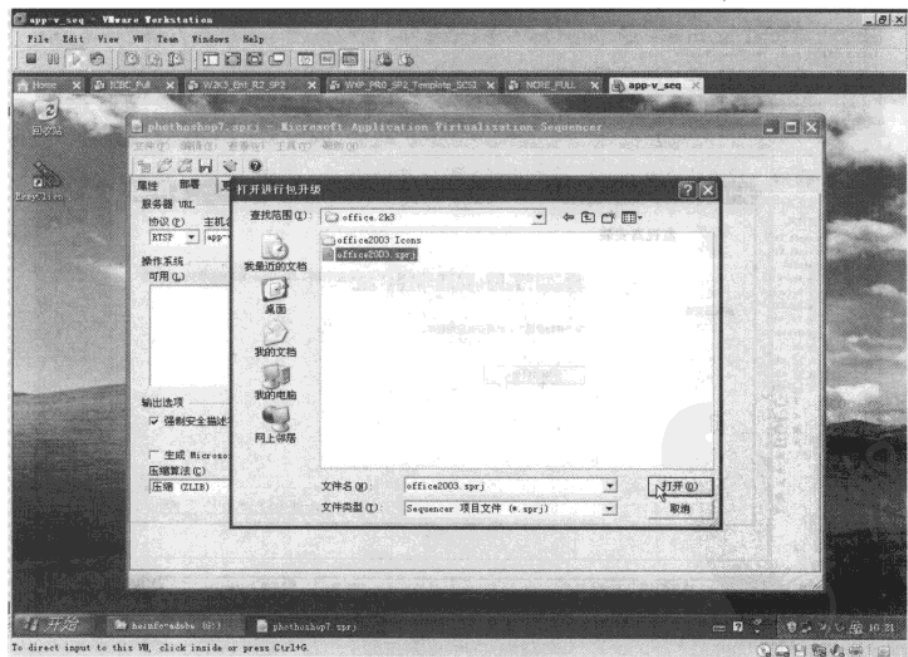


图 3-97 打开封装后的包

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第3步，在“工具”菜单选择“序列化向导”命令，如图3-98所示。

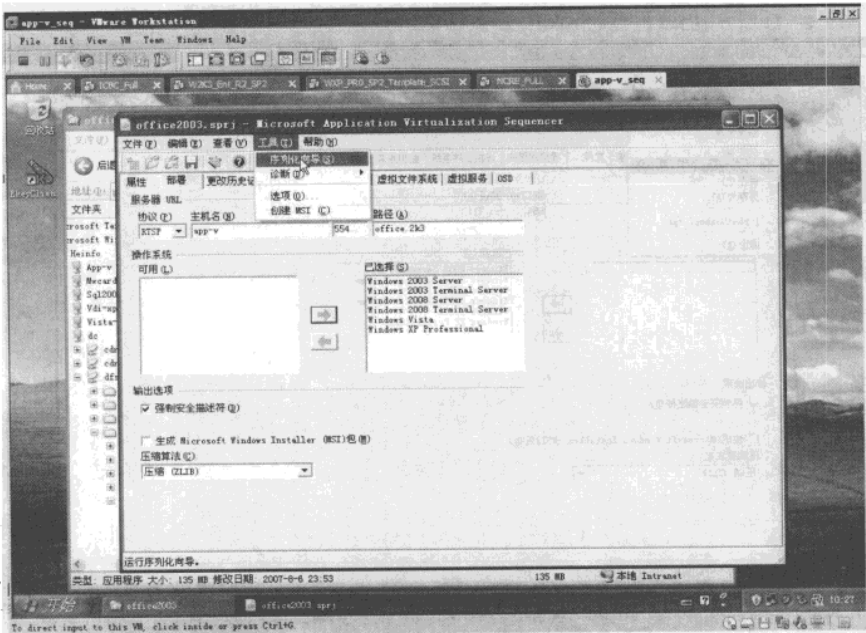


图 3-98 序列化向导

第4步，在“监视器安装”页中，单击“开始监视”按钮，如图3-99所示。

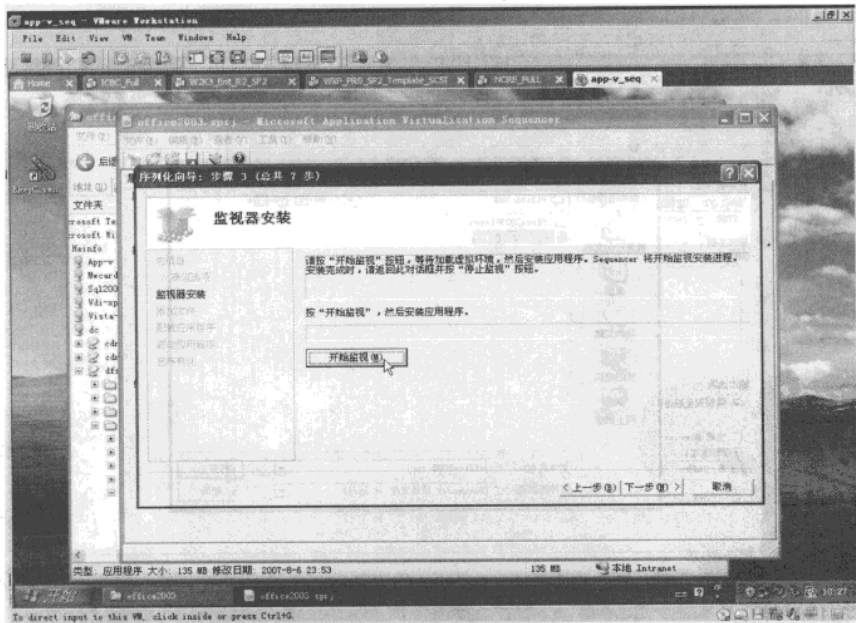


图 3-99 开始监视

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 5 步，运行 Office 2003 SP3 升级程序，如图 3-100 所示。

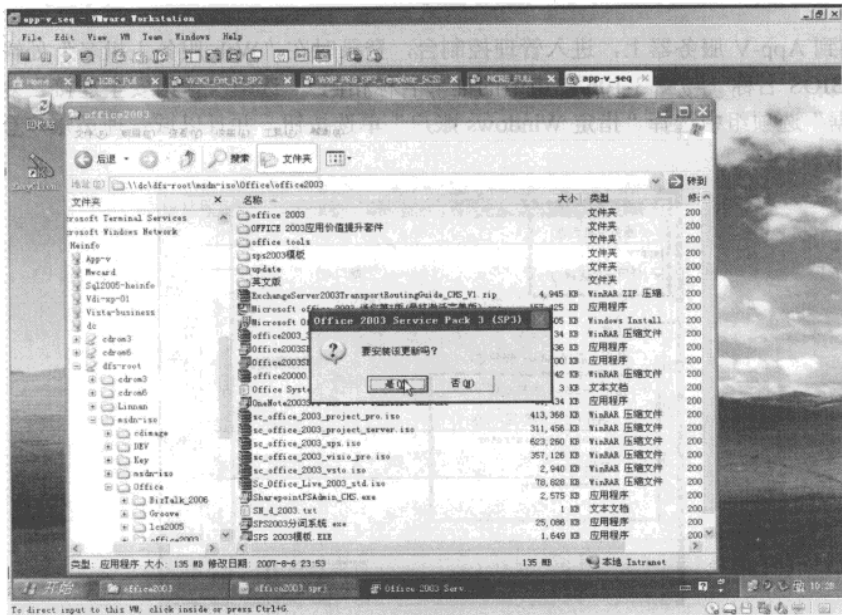


图 3-100 升级 Office 2003 SP3

第 6 步，升级完成后，重新封装，并保存到 App-V 服务器原路径中，如图 3-101 所示。在打包完成后，需要转到 App-V 服务器，导入应用程序，并发布到客户端使用。

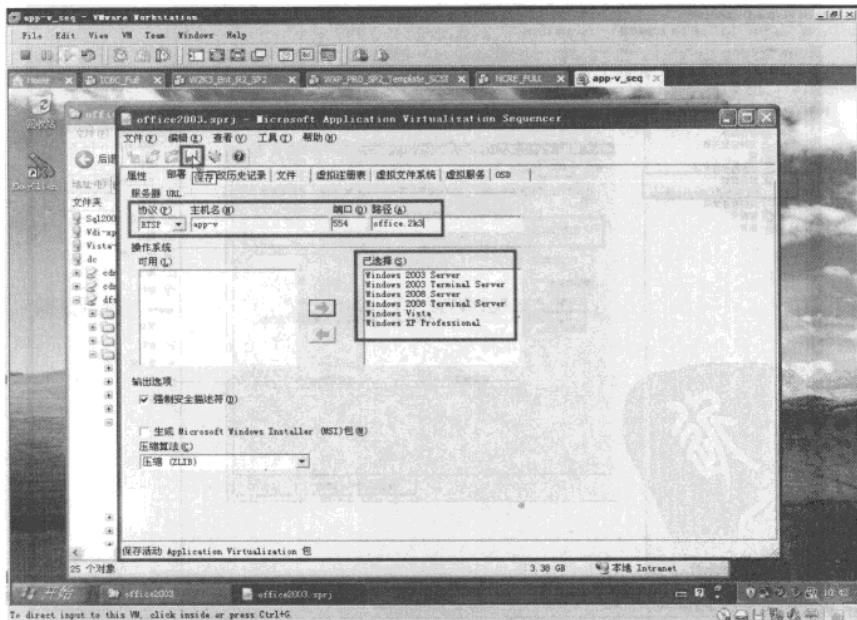


图 3-101 保存到原路径

5. 在 App-V 服务器端导入应用程序

切换到 App-V 服务器上，进入管理控制台，登录时在“Web 服务主机名”处输入当前计算机 NetBIOS 名称（与图 3-106 中申请的证书名称相同），选中“使用安全连接”复选框，在“登录凭据”选项组中选择“指定 Windows 账户”单选按钮，并且以域管理员账户登录，如图 3-102 所示。

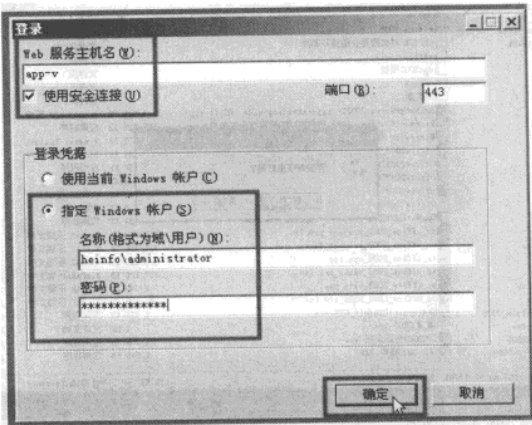


图 3-102 以域管理员账户登录

检查“服务器组→Default Server Group”中，默认的 App-V 服务器组中的服务器，在“端口”中，使用了 RTSP 端口，如图 3-103 所示。

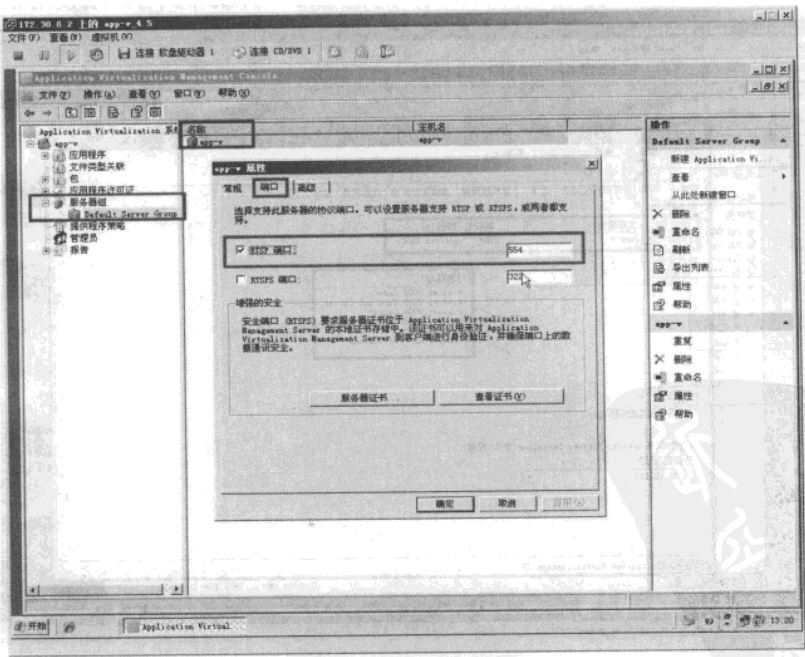


图 3-103 默认服务器组

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有注明来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

在此不需要选中 RTSPS 端口，即使选中，客户端也不能使用 RTSPS 端口。所以，在图 3-95 中封装的时候，选择的服务器使用 RTSP，而不是 RTSPS。注意图 3-102、图 3-95、图 3-93 的计算机名称都是 App-V。

6. 导入打包后的应用程序的步骤

第 1 步，新建“应用程序组”，例如，可以创建 Office 2003、Office 2007、Adobe 等应用程序组，如图 3-104 所示，并且在对应的组导入相应的应用程序。例如，需要在 Office 2003 组导入封装后的 Office 2003 的应用程序。

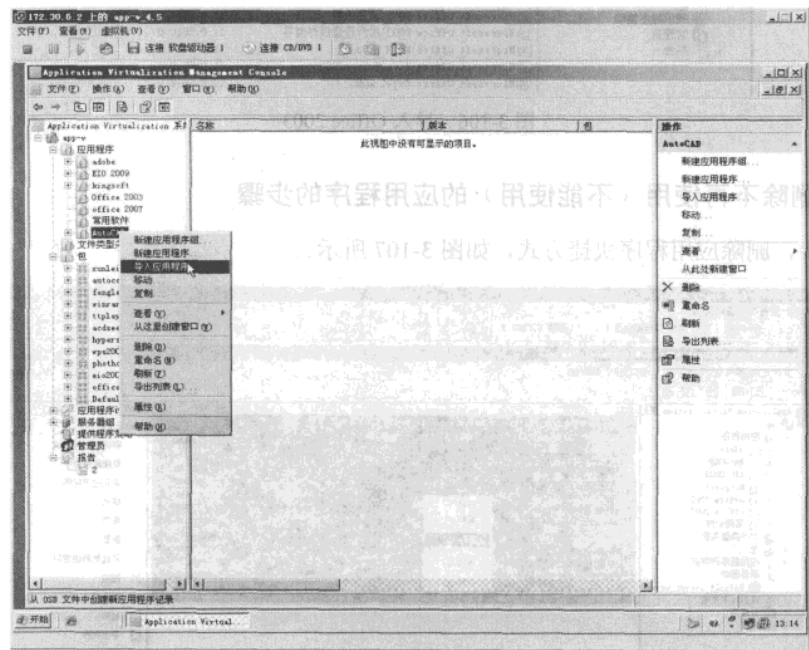


图 3-104 导入应用程序

第 2 步，导入之后，选择应用程序服务器、设置 App-V 用户组，在此不再多说。
第 3 步，导入成功之后的效果如图 3-105 和图 3-106 所示。

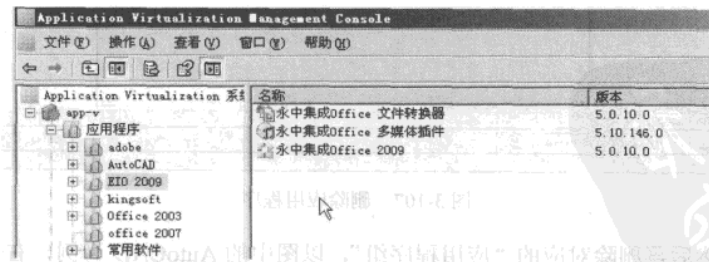


图 3-105 导入永中 Office 2009

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

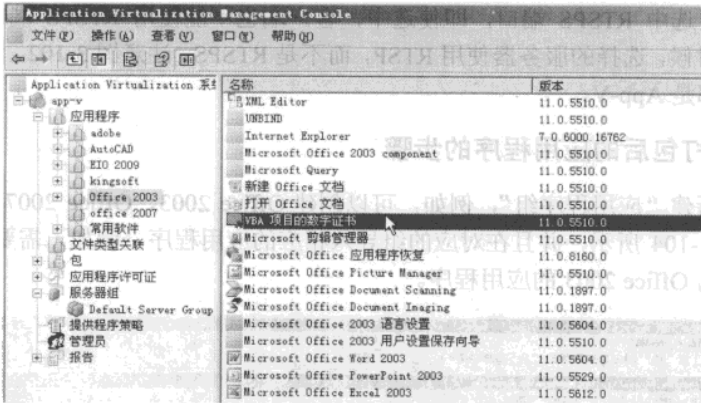


图 3-106 导入 Office 2003

7. 删除不再使用（不能使用）的应用程序的步骤

第 1 步，删除应用程序快捷方式，如图 3-107 所示。

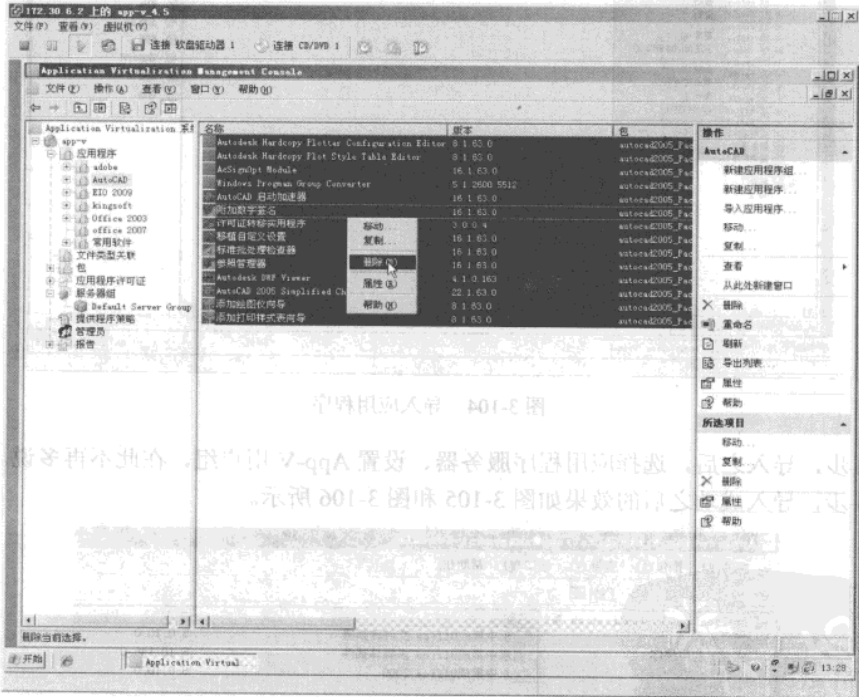


图 3-107 删除应用程序

第 2 步，然后再删除对应的“应用程序组”，以图中的 AutoCAD 为例，右击要删除的包，在弹出的快捷菜单中选择“删除”命令，如图 3-108 所示。

第 3 步，在“content”文件夹下删除封装后的程序包，如图 3-109 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

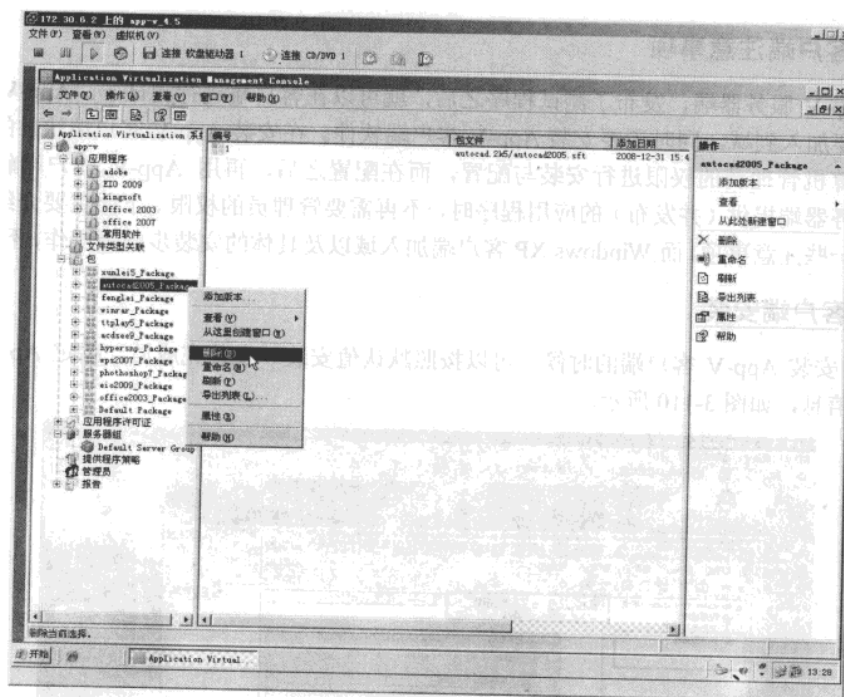


图 3-108 删除包

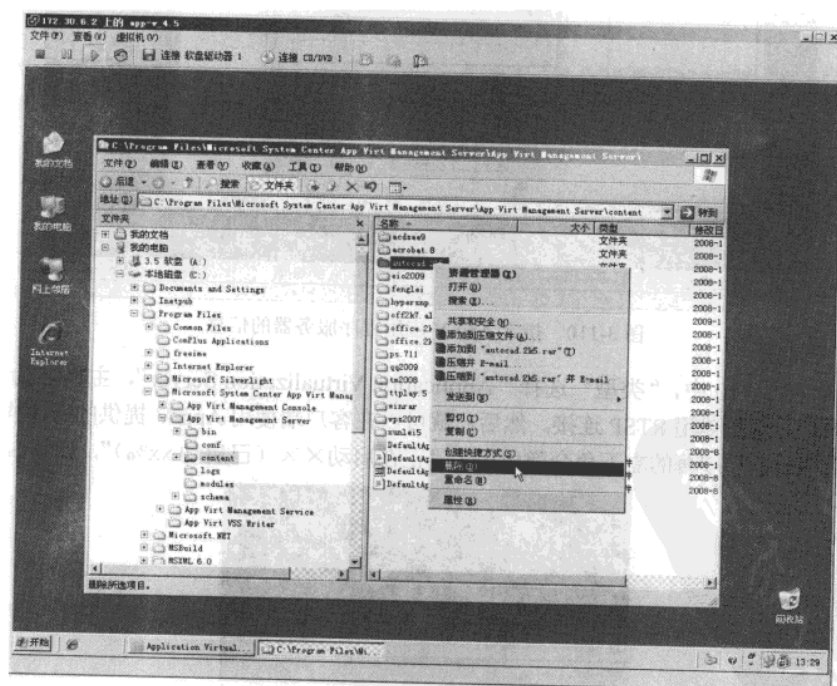


图 3-109 删除封装后的程序包

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8. 客户端注意事项

在 App-V 服务器端，发布了测试程序之后，就可以在客户端进行测试了。App-V 客户端计算机需要加入到域，同时还要安装 App-V 客户端软件。在安装 App-V 客户端软件的时候，必须以计算机管理员的权限进行安装与配置，而在配置之后，再用 App-V 客户端软件使用 App-V 服务器端提供（并发布）的应用程序时，不再需要管理员的权限。下面主要介绍 App-V 客户端的一些注意事项，而 Windows XP 客户端加入域以及具体的安装步骤等操作，不做介绍。

9. 客户端安装

(1) 安装 App-V 客户端的时候，可以按照默认值安装。安装完成后，指定 App-V 服务器的相关信息，如图 3-110 所示。

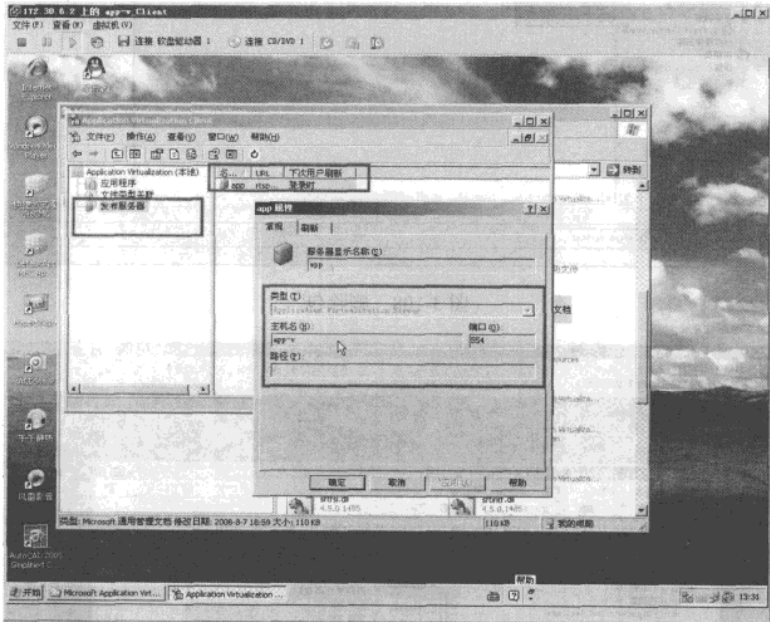


图 3-110 指定 App-V 应用程序服务器的信息

(2) 在图 3-110 中，“类型”选择“Application Virtualization Server”，主机名为“app-v”，端口为“554”。这是使用 RTSP 连接。然后，就可以在客户端使用 App-V 提供的应用程序了。在启动应用程序时，在屏幕的右下角会弹出提示“正在启动××（已启动 xx%）”，如图 3-111 所示。

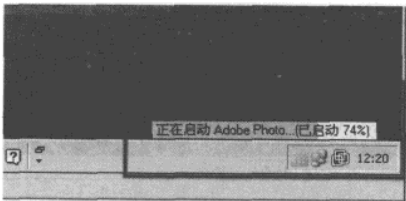


图 3-111 启动进度条

10. App-V 客户端的应用经验

(1) 经过测试，App-V 可以使用大部分应用程序，例如 Office 系列、迅雷、金山 WPS 2007、永中 Office 2009、下载快车、千千静听、风雷影音、Photoshop、Acrobat 等，不能使用 VB、VC、VF、SQL Server，其中 VB 等程序不能安装，SQL Server 可以安装、序列化，但在客户端不能启动。另外，AutoCAD 2005 可以封装，但在客户端使用的时候，出现错误。

另外，根据测试，虽然序列化时、在客户端使用时，QQ2009、TM2008 没有错误，但登录时，提示“网络错误”，这个应该是 QQ 软件的问题（现在没有经过安装的 QQ 是不能登录的）。

(2) 同一产品的不同版本可以同时使用，例如图 3-112 中，Office 2003、Office 2007 同时使用时的界面。

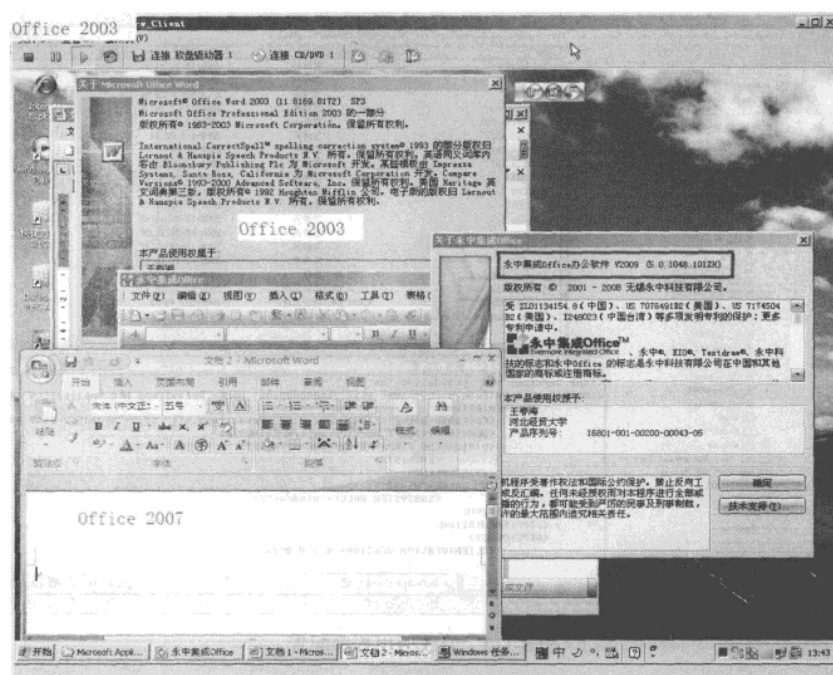


图 3-112 Office 2003、Office 2007 同时运行界面

(3) App-V 客户端，必须有足够的磁盘空间用于缓存。例如，如果磁盘可用空间比较小，在加载 Office 2007 等大程序时，可能会出现磁盘空间不够的错误。

(4) App-V 整个系统，可以用于企业、机关、事业单位，以及部分用于学校的机房。这样，只要客户端操作系统没有问题、客户端加入域、在安装了 App-V 客户端程序时，如果用户需要那种程序，只要使用 App-V 序列化工具进行封装、并在应用程序服务器导入后，客户端在下次登录后就可以使用（或者在图 3-110 中单击刷新按钮）。

(5) 将 App-V 客户端与组策略发布软件结合，可以解决客户端软件部署的问题。而 App-V 的客户端在运行应用软件时，登录 Acdsee、Office 等，不需要具有“本地管理员权限”，只要

网管天下 网管经验谈

具有“普通用户”权限即可。

(6) App-V 的客户端，只有在使用某个应用程序时，才“自动”从 App-V 应用程序服务器下载序列化后的软件到本地、同时加载与软件对应的“虚拟注册表”到虚拟环境中运行，当软件关闭后，同时关闭相应的虚拟环境。从这一点来看，不管是在 App-V 客户端运行那款软件，运行之后是“绿色”的，不对计算机本身的注册表进行修改。这样，由于客户端运行时，只需要加载 App-V 的客户端，并不需要加载其他的软件。

(7) 如果要测试 App-V 自带的应用程序，使用“记事本”打开 Defaultapp.osd 程序，将默认的 RTSPS 修改为 RTSP，并且将端口从 322 改为 554，如图 3-113 所示。

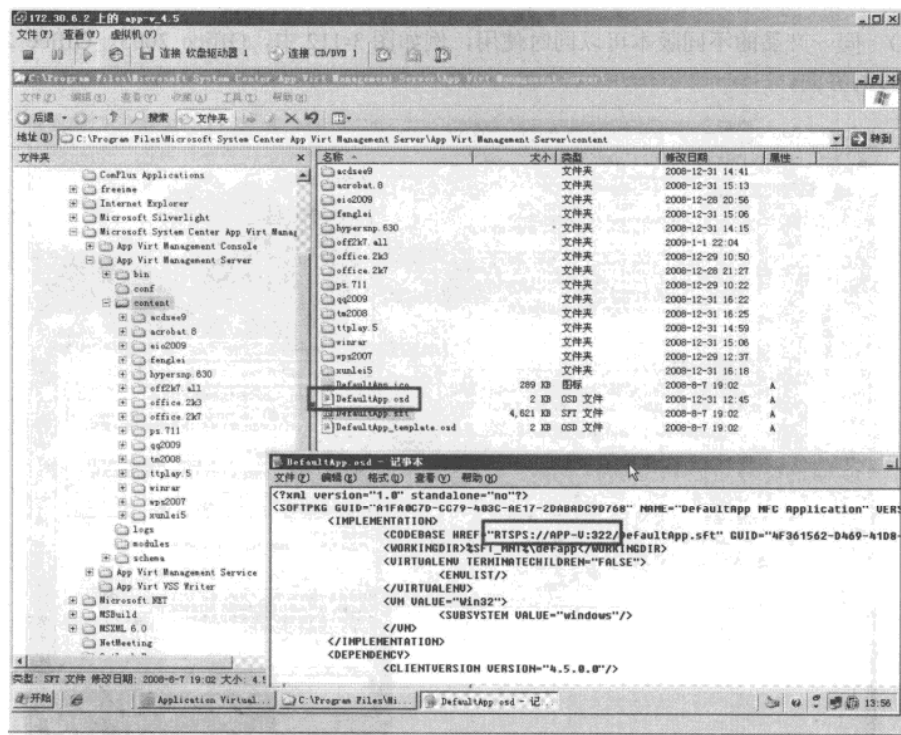


图 3-113 修改应用程序配置

3.4.2 域环境安装企业根 CA 经验

- (1) 环境：在域环境下一台 DC 域控制器，IP 地址：172.21.21.21。
- (2) 要求：安装企业根 CA，申请一个用户证书。
- (3) 具体步骤：
第 1 步，在 DC 服务器先安装 IIS，再安装证书服务，如图 3-114 所示。
第 2 步，在 Windows 组件向导选择“证书服务”复选框，单击“是”按钮确定安装，如图 3-115 所示。
第 3 步，在“证书服务”前已经打上了对勾，如图 3-116 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

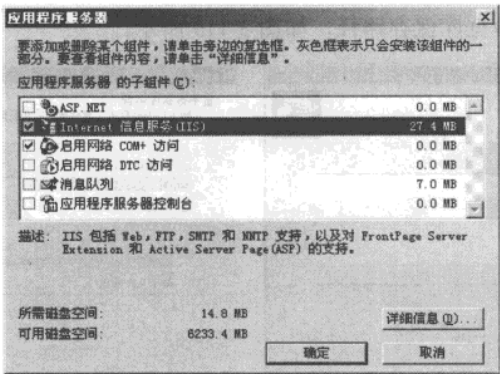


图 3-114 安装 IIS

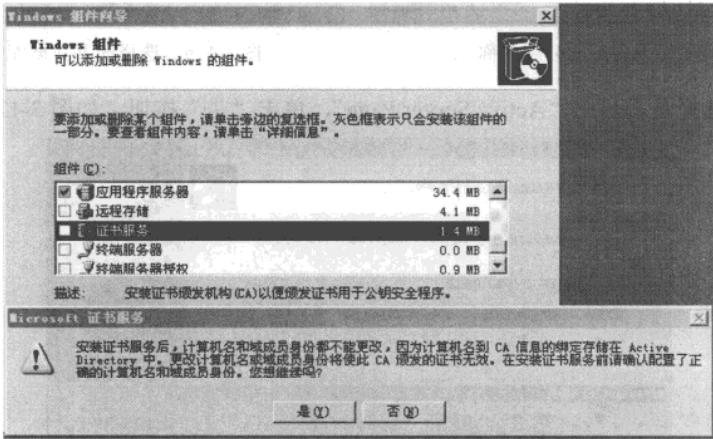


图 3-115 安装证书服务

第 4 步，选择“企业根 CA”单选按钮，如图 3-117 所示。

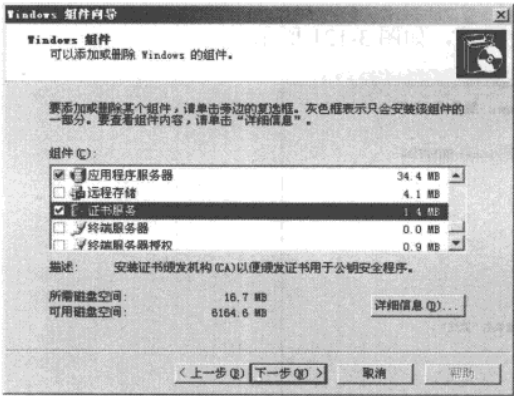


图 3-116 确定安装证书服务

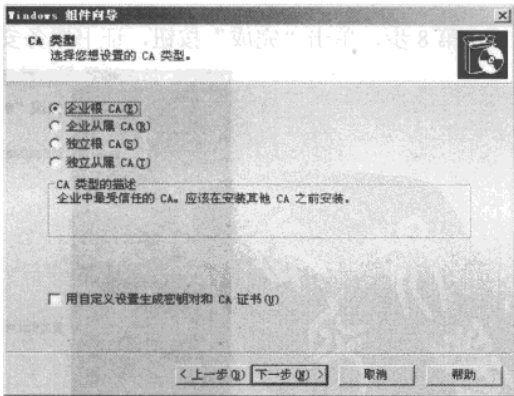


图 3-117 选择企业根 CA

第 5 步，输入 CA 的公用名称，可以自定义，如图 3-118 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 6 步，选择证书数据库保存路径，如图 3-119 所示。

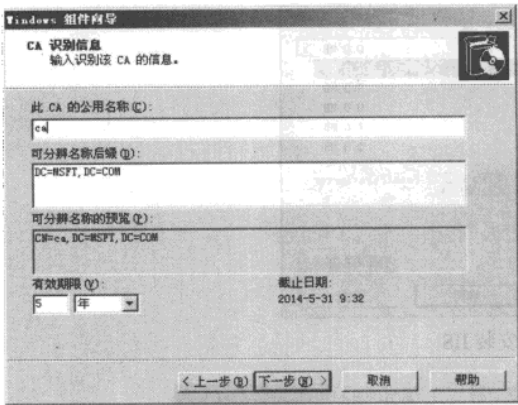


图 3-118 输入 CA 的公用名称

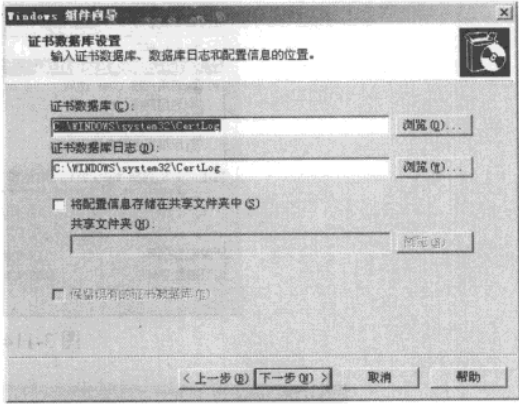


图 3-119 选择证书数据库保存路径

第 7 步，选择是否启用“Active Server Page”，单击“是”按钮，如图 3-120 所示。

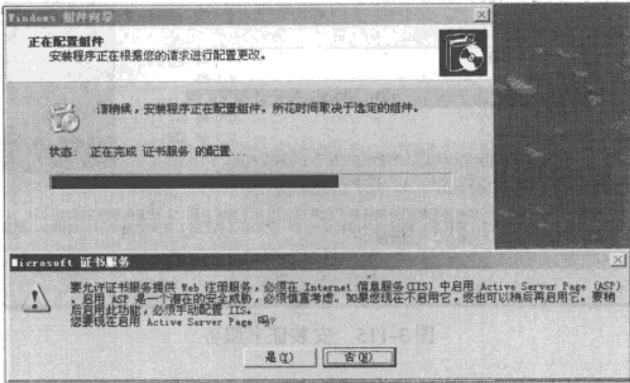


图 3-120 启用“Active Server Page”

第 8 步，单击“完成”按钮，证书服务安装成功，如图 3-121 所示。

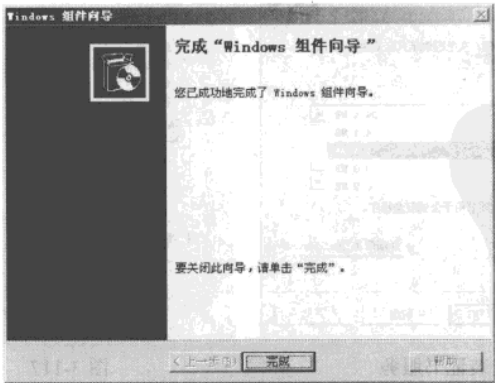


图 3-121 完成证书服务的安装

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

至此，证书服务已经安装完毕。下面我们来申请一个可用的证书。
第 1 步，打开“证书颁发机构”如图 3-122 所示。

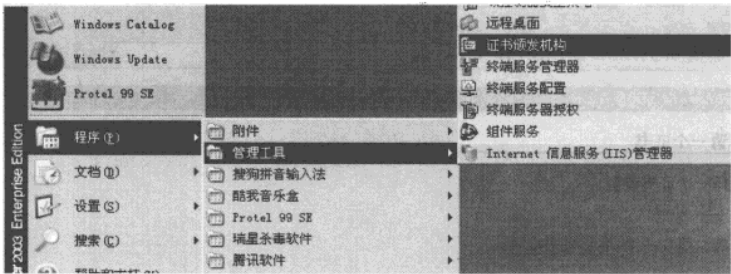


图 3-122 打开证书颁发机构

第 2 步，可以选择“停止证书服务”和“启动证书服务”，如图 3-123 和图 3-124 所示。

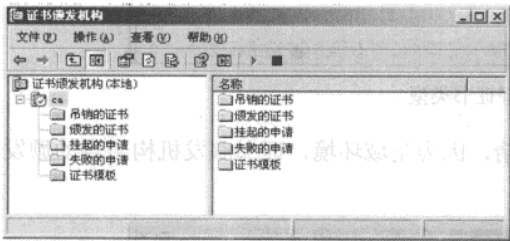


图 3-123 停止证书服务

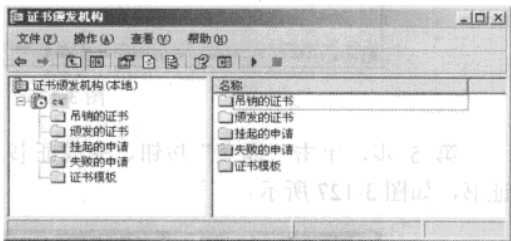


图 3-124 启动证书服务

第 3 步，在客户端打开 IE，输入证书申请网站，用域账号登入去申请用户证书，如图 3-125 所示。

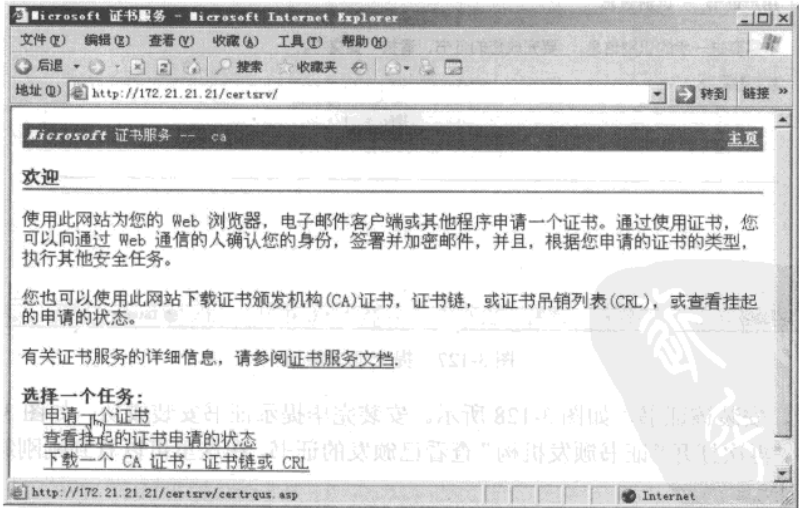


图 3-125 打开证书申请网站

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 4 步，选择证书类型，如图 3-126 所示。

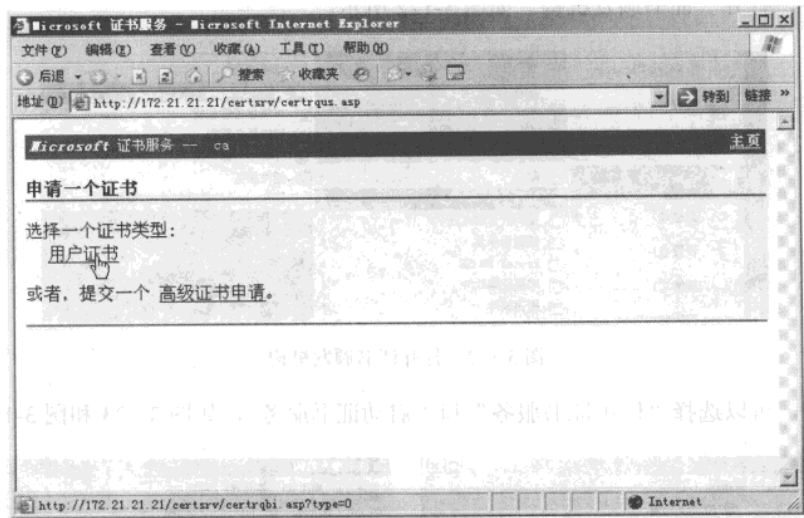


图 3-126 选择证书类型

第 5 步，单击“提交”按钮，完成证书申请，因为是域环境，证书颁发机构会自动颁发证书，如图 3-127 所示。

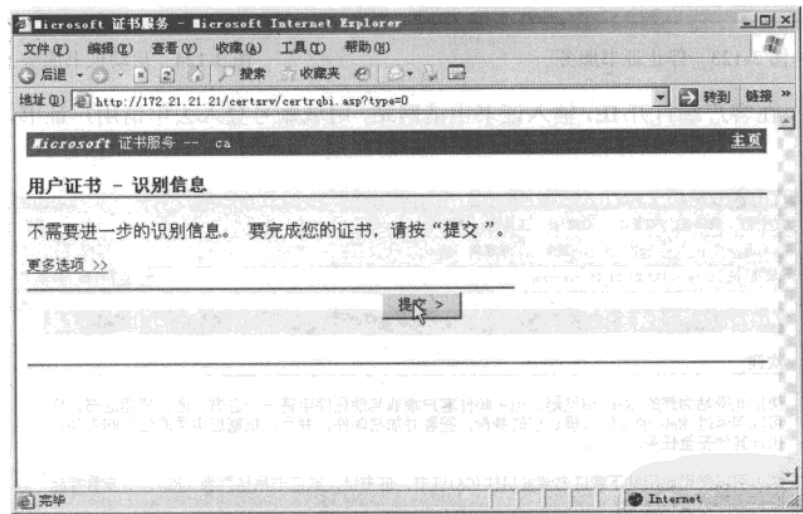


图 3-127 提交证书申请

第 6 步，安装该证书，如图 3-128 所示。安装完毕提示证书安装成功，如图 3-129 所示。
第 7 步，再次打开“证书颁发机构”查看已颁发的证书，在这里可以看到刚刚颁发的证书，如图 3-130 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

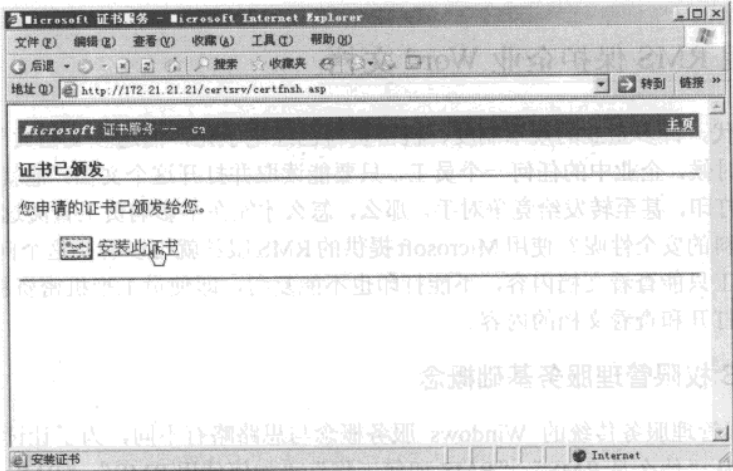


图 3-128 安装证书

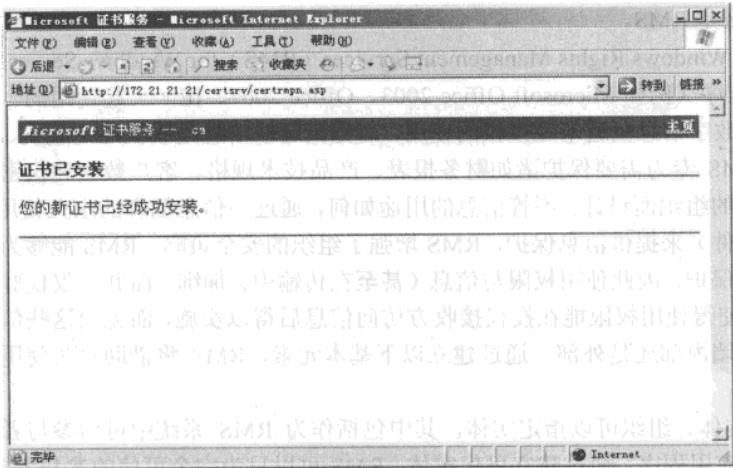


图 3-129 证书安装成功

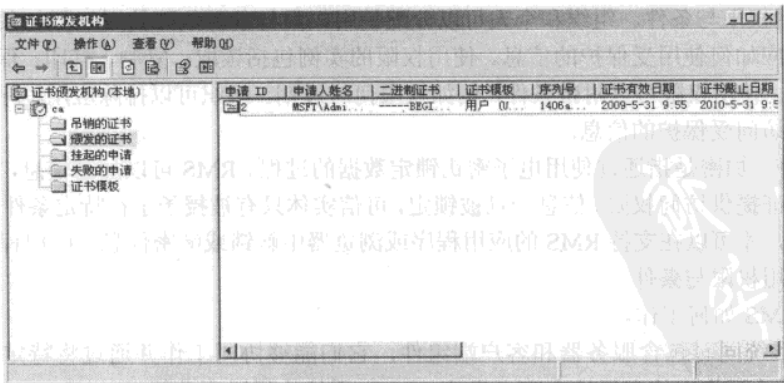


图 3-130 查看颁发的新证书

3.4.3 使用 RMS 保护企业 Word 文档

在信息时代，许多企业的规章制度、机密资料已经电子化，而这些文档大部分又是 word 文档。在许多时候，企业中的任何一个员工，只要能读取并打开这个文档，他就可以把这些重要资料复制、打印，甚至转发给竞争对手。那么，怎么才能在不影响员工查阅这些资料的同时又确保这些资料的安全性呢？使用 Microsoft 提供的 RMS 服务就可以解决这个问题，使用 RMS 服务，企业员工只能查看文档内容，不能打印也不能复印，即使员工把机密资料发送给他人，其他人也不能打开和查看文档的内容。

1. RMS 权限管理服务基础概念

RMS 权限管理服务传统的 Windows 服务概念与思路略有不同，为了让读者熟悉并应用 RMS，本节将从“什么是 RMS”、“RMS 如何工作”、“如何使用 RMS”、“RMS 的系统需求”、“客户端访问许可证要求”等几个方面介绍。

(1) 什么是 RMS。

Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 是与支持 RMS 的应用程序（例如 Microsoft Office 2003、Office 2007、IE）一起使用的一种信息保护技术，可以保护数字信息免遭未经授权的使用，而无论这些信息是联机还是脱机、在防火墙内部还是外部。RMS 专为需要保护诸如财务报表、产品技术规格、客户数据和机密电子邮件等敏感及专有信息的组织而设计。不管信息的用途如何，通过与信息捆绑的永久使用策略（也称为使用权限与条件）来提供信息保护，RMS 增强了组织的安全策略。RMS 能够为二进制格式的数据提供永久保护，因此使用权限与信息（甚至在传输中）捆绑，而并非仅仅驻留在组织的网络中。这样也使得使用权限能在授权接收方访问信息后得以实施，而无论这些信息是联机还是脱机、在防火墙内部还是外部。通过建立以下基本元素，RMS 将借助永久使用策略帮助你保护信息：

① 可信实体。组织可以指定实体，其中包括作为 RMS 系统中可信参与者的个人、用户组、计算机和应用程序。通过建立可信实体，RMS 可以只为完全可信的参与者授予访问权限，从而对信息提供保护。

② 使用权限与条件。组织和个人可以分配使用权限与条件，而使用权限与条件定义了特定可信实体应如何使用受保护的信息。使用权限的实例包括读取、复制、打印、保存、转发和编辑的权限。使用权限可以附带条件，例如权限何时过期。组织可以排除应用程序和实体，从而使其无法访问受保护的信息。

③ 加密。加密是指通过使用电子密钥锁定数据的过程。RMS 可以加密信息，根据可信实体的成功验证提供访问权限。信息一旦被锁定，可信实体只有被授予了在特定条件下（如果有）的使用权限，才可以在支持 RMS 的应用程序或浏览器中解锁或解密信息。应用程序随后将实施定义的使用权限与条件。

(2) RMS 如何工作。

RMS 系统同时包含服务器和客户端组件，它们能够协同工作并通过将特定权限仅授予 RMS 系统中的可信实体来保护内容。为此，RMS 系统执行以下功能：

① 创建受 RMS 保护的文件和容器。RMS 系统中的可信实体用户可以通过使用熟悉的、

支持 RMS 的创作应用程序和工具，轻松创建和管理受保护的文件。Microsoft Office 2003 即是支持 RMS 的应用程序之一。用户可以使用支持 RMS 的应用程序对内容应用使用权限与条件，即创建“受保护内容”。此外，RMS 还为 RMS 管理员提供了定义模板的功能，这些模板可以为受保护内容授予某些预定义权限集（例如“公司机密”）。创建模板后，必须配置支持 RMS 的应用程序以使用这些模板。

② 验证用户并授权受 RMS 保护的信息。由 RMS 系统颁发的权限账户证书用于标识可发布或查看受 RMS 保护的信息的可信实体。RMS 系统中的可信实体用户可以使用支持 RMS 的应用程序为要保护的信息指定使用权限与条件。这些使用策略指定哪些用户可以使用该信息，以及用户可以对该信息执行哪些操作。

RMS 系统验证可信实体，并颁发包含针对该信息的指定使用权限和条件的发布许可证。该信息将通过使用支持 RMS 的应用程序以及可信实体的权限账户证书中的电子密钥进行加密。使用此机制将信息加密或锁定之后，只有在发布许可证中指定的可信实体才能解锁并使用该内容。

③ 获取许可证以解密受 RMS 保护的信息并实施使用策略。通过使用可信计算机和应用程序，可信实体接收方可以打开或查看受 RMS 保护的信息。这些支持 RMS 的应用程序将实施由信息作者定义的使用权限。包含用于加密信息的公钥的 RMS 服务器将验证接收方的凭据，然后颁发包含在发布许可证中指定的使用权限与条件的用户许可证。该信息将通过使用可信实体的用户许可证和权限账户证书中的电子密钥进行解密。支持 RMS 的应用程序随后将实施使用权限与条件。每次打开该内容时，支持 RMS 的客户端将检查用户是否仍具有查看内容的权限。在权限账户证书或计算机证书已过期、发布许可证中指定的证书已被吊销或内容已过期等情况下，用户将失去打开内容的权限。

（3）如何使用 RMS。

不同的组织中可能存在多种不同的 RMS 应用程序，以下方案提供了关于如何在组织中使用 RMS 的一些应用。

方案 1：保护机密电子邮件。公司经理需要向项目小组发送机密电子邮件，其中附带关于新项目的文档。公司的 IT 部门使用 RMS 创建了“公司机密”权限策略模板，该模板将自动应用 RMS 服务器中定义的使用权限。经理可以选择该模板为电子邮件添加使用权限，而电子邮件将自动对附带的文档应用相同的权限。“公司机密”模板指定了只有组织内部雇员才能阅读该信息。当雇员打开电子邮件及附件时，支持 RMS 的应用程序将验证用户并执行对信息的使用权限。根据“公司机密”模板中指定的使用权限，雇员将无法复制、保存或编辑该电子邮件或附件文档，同时也不能转发该电子邮件。如果用户尝试向组织外部转发电子邮件或附件，未经授权的接收方将无法打开该信息。

方案 2：与可信合作伙伴共享受保护的内容。在收到上述的电子邮件和项目计划之后，小组成员可以向经理（即文档所有者）发送请求，要求获得与项目的外部供应商共享电子邮件及附件的权限。对 RMS 解决方案使用宿主提供商的供应商在公司的 RMS 环境中属于可信合作伙伴。经理可以对供应商应用相应的权限，然后再向该供应商发送电子邮件。当供应商收到并打开电子邮件及附件时将执行更新后的使用权限。

方案 3：执行文档权限。北京的一位剧本作家使用支持 RMS 的应用程序中的权限选项为剧本设置了使用权限，以便与上海办事处的一位制片人共享该剧本。该剧本作家将剧本发送到了内部文件共享服务器上供制片人访问。在发送剧本后，剧本作家向该制片人发送了一封电子

网管天下 网管经验谈

邮件，在邮件中提供了该文件在文件服务器上的位置。根据作家为文档设置的使用权限，制片人可以在一周内查看和编辑剧本。该制片人将文档下载到了自己的便携式计算机并打开进行评改。在一周内，制片人可以随时处理该文档，而不必连接至文件服务器、内部网络或 Internet。一旦授权她使用文档，许可证在到期日期之前将始终有效。

但在一周之后，该制片人觉得自己还需要更多的时间来评改剧本，而此时她已无法打开该文档。因此，她请求作家延长时间以继续评改剧本。于是，制片人将已过期的文档连同自己的评改一道发给该作家，以便更新文档的到期日期。一旦作家更新了到期日期，制片人便可以下载更新版本并继续评改和编辑该剧本。

方案 4：保护敏感的 Intranet 内容。一家大型跨国出版社的销售经理及其整个销售组织需要查看存储在公司 Intranet 联机系统中的销售业绩。出于信息敏感性的考虑，公司决定对销售业绩应用使用权限。在本示例中，公司对信息应用了“只读”权限，允许销售组织查看销售业绩但不能修改、复制、导出、保存或打印信息。与此同时，需要复制或打印销售业绩的管理人员被授予了增强权限，以便他们将销售业绩用于演示和商业评论。

说明 在方案 4 中，支持 RMS 的应用程序为支持 RMS 的浏览器，例如 Internet Explorer。

2. 在企业网络中部署 RMS 服务

RMS 主要用于使用 Active Directory 进行管理的企业网络中，本节将在一个真实的网络环境中部署 RMS 并介绍其应用。本节的网络环境，如表 3-3 所示。

表 3-3 RMS 权限管理服务器部署环境

计算机名	IP 地址	作用	备注
ad-server	172.30.5.3	Active Directory 服务器	域名为 labs.yijiao
server-dhcp	172.30.5.5	RMS 服务器	将要部署为 RMS 服务器
Exchange	172.30.5.15	Exchange 邮件服务器	也可以使用其他邮件系统
SPS2003	172.30.5.11	SQL Server 2005 数据库服务器	也可以使用 SQL2000、MSDE 2000 等数据库

- 其网络拓扑如图 3-131 所示。
- RMS 服务器需要如下的环境（或组件支持）：
- Active Directory 目录服务。
 - Microsoft Internet 信息服务 6.0（IIS）。
 - Microsoft SQL Server 2000、SQL Server 2005 或 MSDE。
 - 需要具有公共密钥基础结构（PKI）的相关知识。
 - RMS 服务器需要连接到 Internet。

下面将介绍部署 RMS 服务器的过程与步骤。

（1）安装 RMS 服务器。

在准备安装 RMS 之前，请确认网络中已经存在 Active Directory 服务器，在本例中，服务器的类型、名称、IP 地址与表 3-3 相同。在安装 RMS 之前，这些服务器都已经安装并配置好。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面将在 IP 地址为 172.30.5.5 的计算机上，安装 RMS 服务器，主要步骤如下。

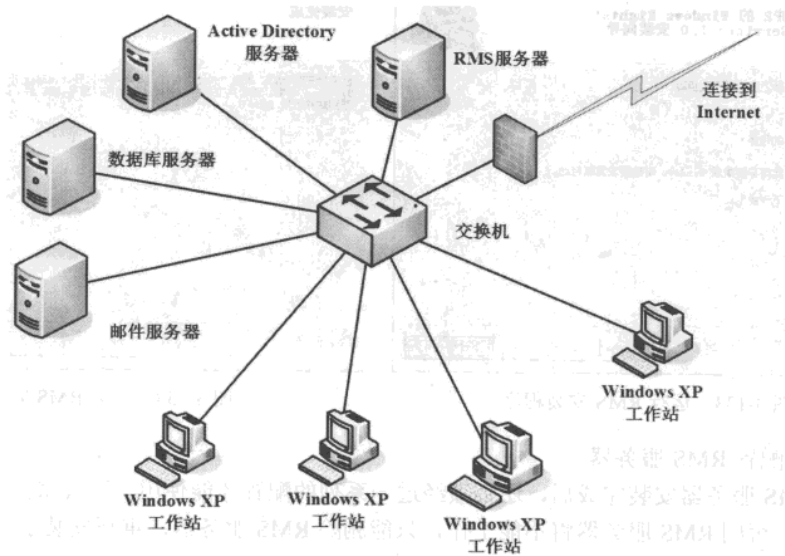


图 3-131 RMS 服务器工作的网络拓扑

第 1 步，在准备安装 RMS 服务器的计算机上，将此服务器加入到 Active Directory，或者使用“dcpromo”命令，将此服务器升级到“labs.yijiao”域的“额外域控制器”，升级之后，以“域管理员”账户登录。

第 2 步，在“添加/删除程序”→“添加 Windows 组件”页中，在“应用程序服务器”中添加“ASP.NET”、“Internet 信息服务”和“消息队列”服务，如图 3-132 所示。

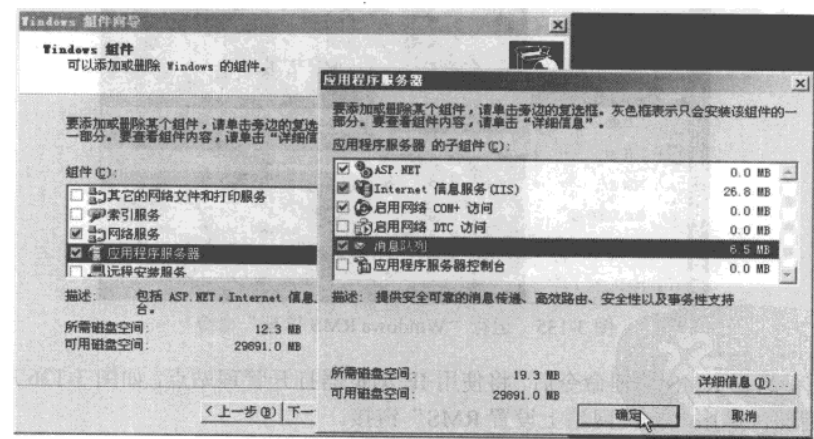


图 3-132 安装 IIS 与消息队列组件

第 3 步，安装 IIS 组件完成后，运行 RMS 的安装程序，如图 3-133 所示。

第 4 步，完全按照默认值安装，直到安装完成，如图 3-134 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

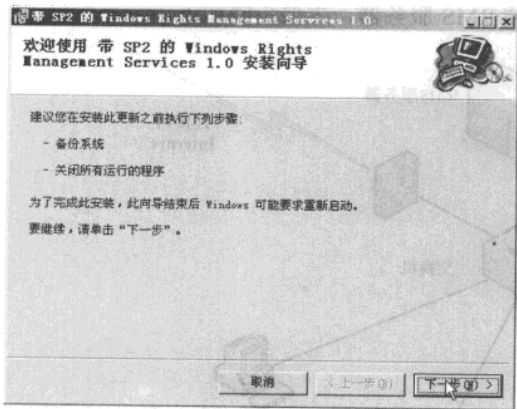


图 3-133 运行 RMS 安装程序

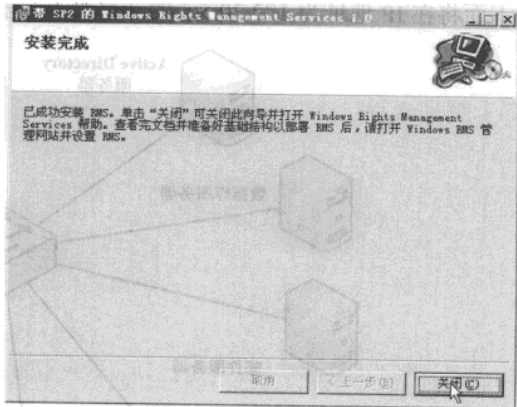


图 3-134 安装 RMS 完成

(2) 配置 RMS 服务器。

当 RMS 服务器安装完成后，还必须经过一系列的配置才能使用，请大家完全按照下面的步骤进行，否则 RMS 服务器将不能工作，只能删除 RMS 服务器，重新安装了。

说·明

必须在安装 RMS 服务器的计算机上进行下面的工作。

第 1 步，从“程序”菜单的“Windows RMS”程序组运行“Windows RMS 管理”命令，如图 3-135 所示。

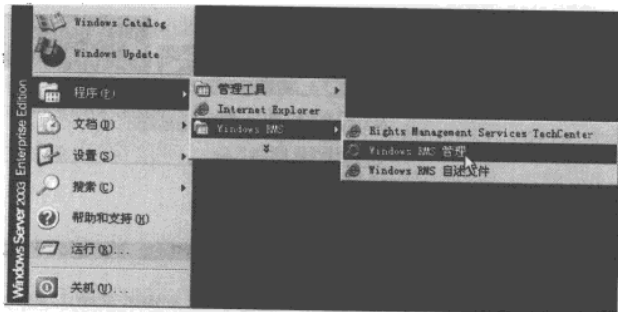


图 3-135 运行“Windows RMS 管理”命令

第 2 步，运行 RMS 管理命令后，将使用 IE 浏览器打开管理站点，如图 3-136 所示。在“默认网站”后面，单击“在此网站上设置 RMS”链接。

注·意

RMS 管理站点只能安装在“默认网站”上，如果将 RMS 管理站点安装在其他网站上，将不能进入管理页面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

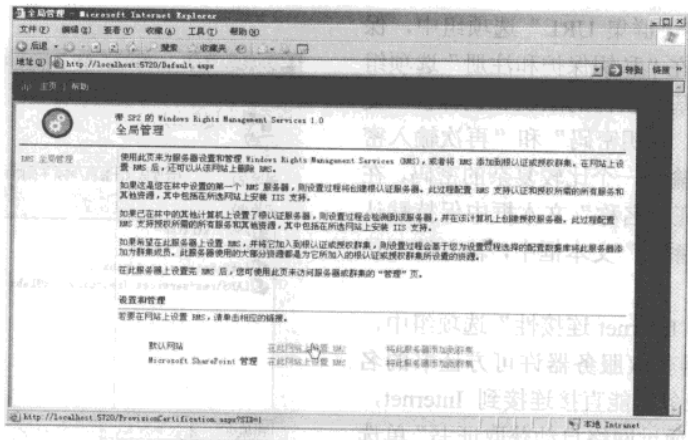


图 3-136 在默认网站上设置 RMS

第 3 步，在“设置 RMS 根认证服务器—默认网站”页中，为 RMS 服务器进行配置，首先需要配置数据库及服务账户，如图 3-137 所示。

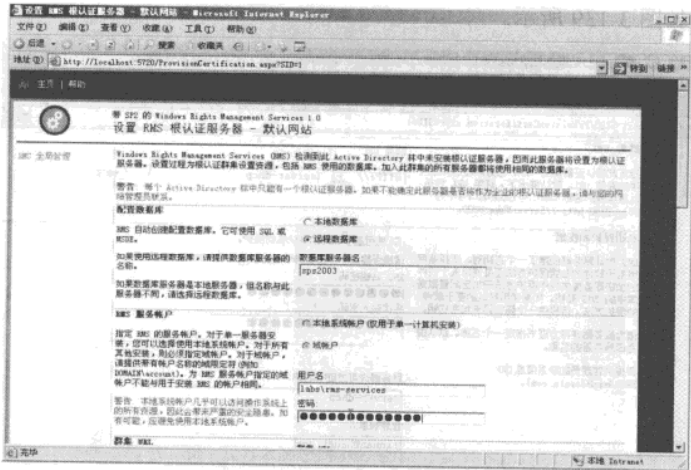


图 3-137 指定数据库服务器位置及 RMS 服务账户名称

在“配置数据库”选项组中，指定 SQL Server 服务器的位置，在本例中，SQL Server 安装在名为“sps2003”的计算机上，所以，在本例中选“远程数据库”单选按钮，并在“数据库服务器名”文本框中输入“sps2003”。

在“RMS 服务账户”选项组中，指定 RMS 服务账户，请返回到“Active Directory 用户和计算机”管理单元，为 RMS 服务器创建一个账户，此账户是一个“域普通用户”即可，在本例中，创建的用户名为 rms-services。

说明 如果安装 RMS 服务器的计算机是 Active Directory 中的一台“成员服务器”，而不是“额外域控制器”，需要将创建的用户添加到 RMS 服务器的“本地管理员”组中，如图 3-138 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 4 步，在“群集 URL”选项组中，保持默认值即可；在“私钥保护和注册”选项组中，选择“使用基于软件的默认私钥保护”复选框，在“RMS 私钥密码”和“再次输入密码”密码框中，输入一个比较复杂的密码，在“服务器许可方证书名称”文本框中保持默认值，在“管理联系人”文本框中，输入管理员的邮箱。

在“服务器 Internet 连接性”选项组中，选择这台服务器获取服务器许可方证书的名称，如果这台服务器能直接连接到 Internet，则单击“脱机—通过网络自动获取证书”单选按钮，如果这台服务器没有连接到 Internet，则选择“脱机—设置后手动获取证书”单选按钮，在本例中，服务器已经连接到 Internet，所以选择前者，如图 3-139 所示。

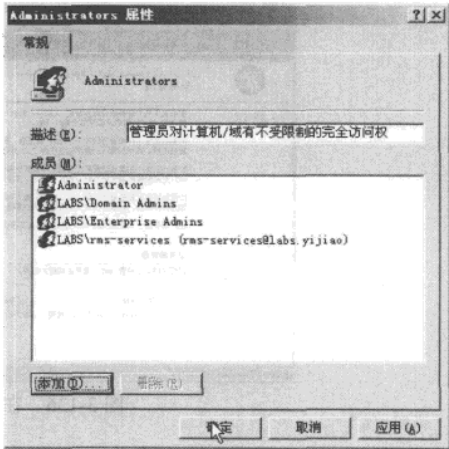


图 3-138 将 RMS 服务账户添加到本地管理员组中

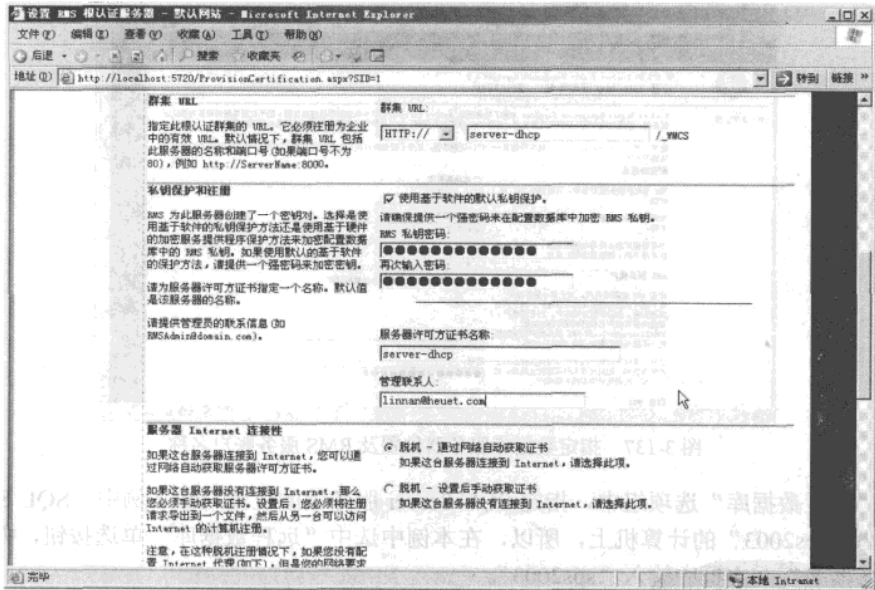


图 3-139 设置私钥保护和选择 Internet 连接性

第 5 步，在“RMS 代理服务器设置”页中，选择连接到 Internet 的方式，如果该服务器直接连接到 Internet，则取消“此计算机使用代理服务器连接到 Internet”复选框，如果该服务器通过代理服务器连接到 Internet，则选中“此计算机使用代理服务器连接到 Internet”复选框并设置代理服务器地址、用户名等信息。

在“吊销”选项组中，保持空白，然后单击“提交”按钮，如图 3-140 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

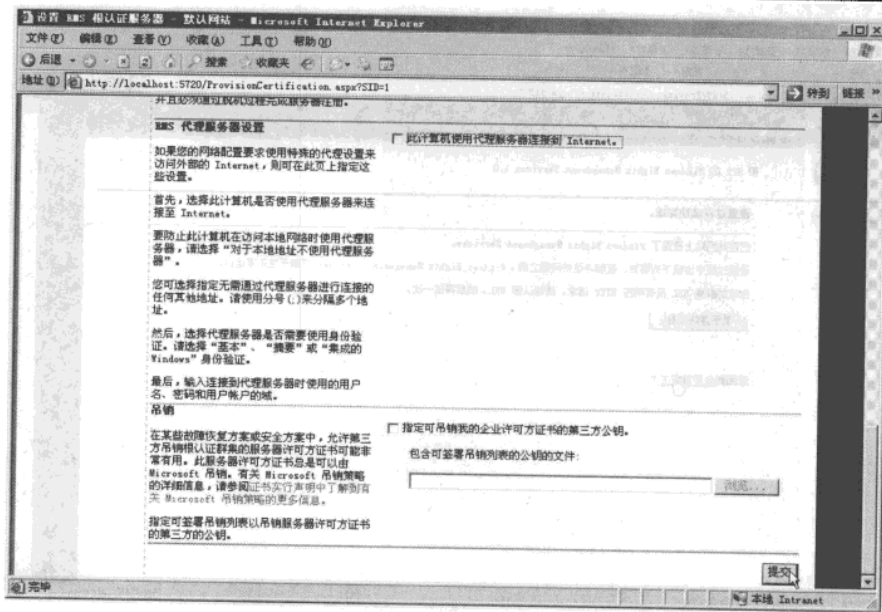


图 3-140 设置连接到 Internet 的方式

第 6 步，单击“提交”按钮后，RMS 服务器将进行配置，这需要五、六分钟的时间，如图 3-141 所示。

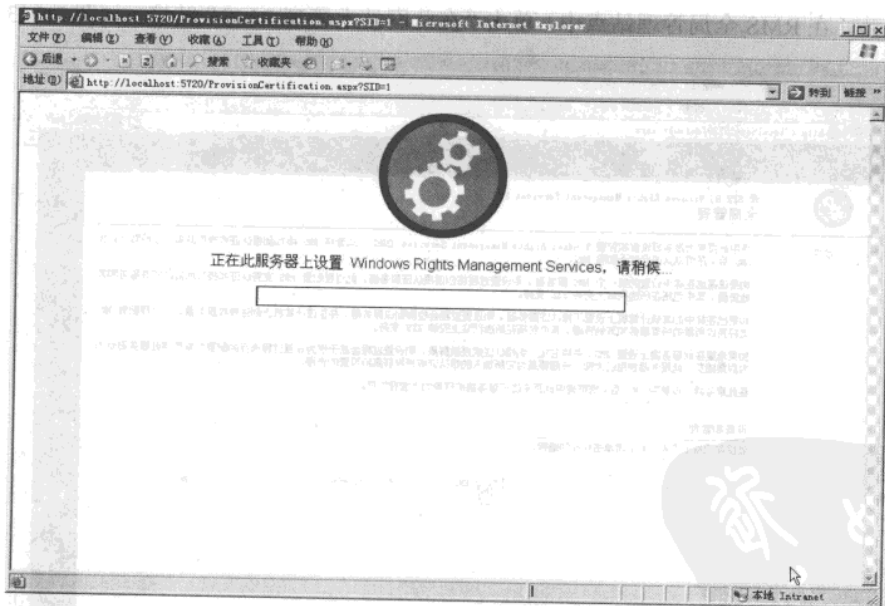


图 3-141 配置 RMS 服务器

第 7 步，RMS 服务器配置完成后，单击“全局管理主页”链接，返回到全局管理页，继续设置，如图 3-142 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

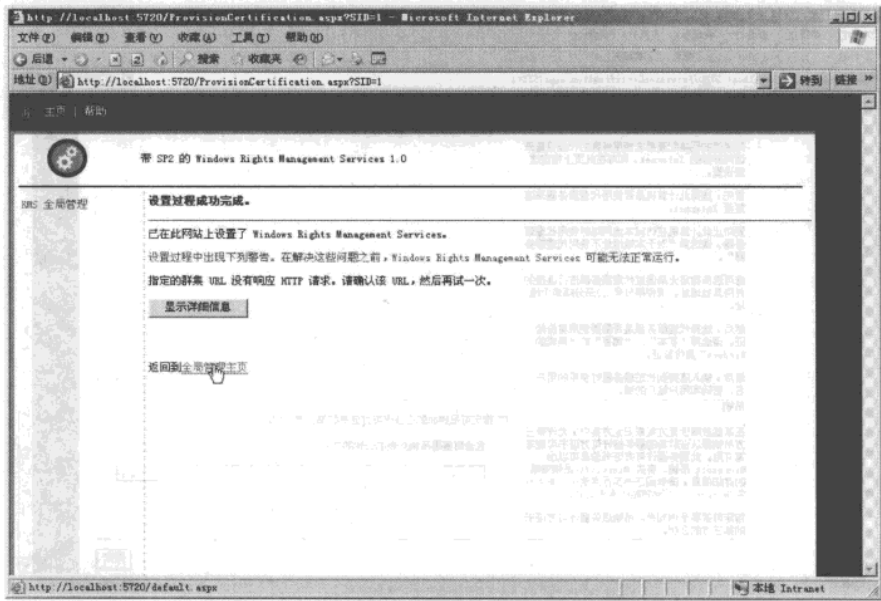


图 3-142 RMS 设置完成

(3) 注册 RMS 服务器。
当 RMS 服务器配置完成后，还必须经过最后的设置才能工作，操作步骤如下：
第 1 步，在 RMS 全局管理站点中，单击“在此网站上管理 RMS”链接，如图 3-143 所示。



图 3-143 管理 RMS

第 2 步，在“管理默认网站”页，单击左下角的“RMS 服务连接点”链接，如图 3-144

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。

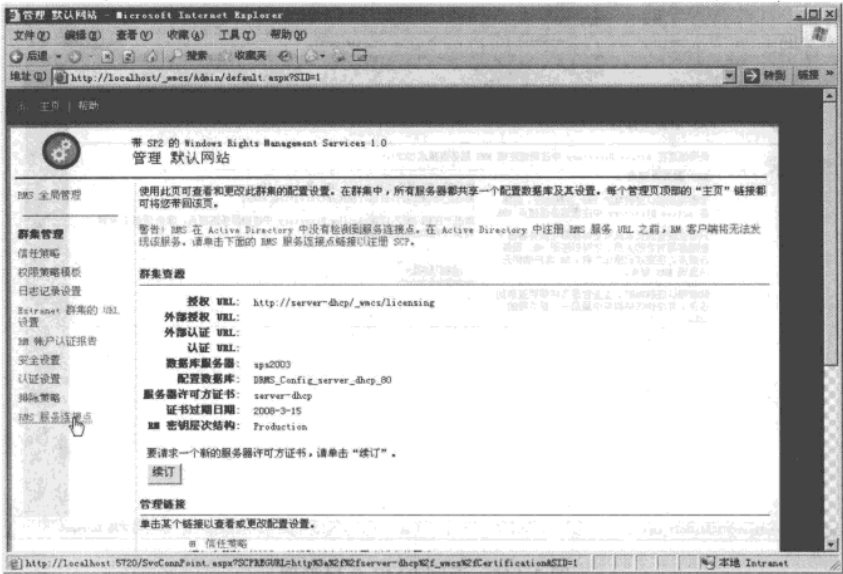


图 3-144 RMS 服务连接点

第 3 步，在“RMS 服务连接点”页中，单击“注册 URL”按钮，如图 3-145 所示。

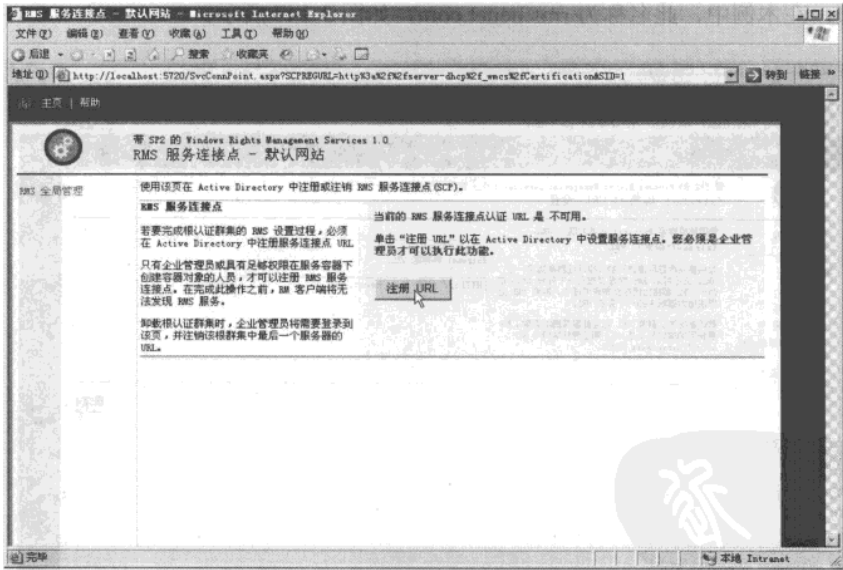


图 3-145 注册 URL

第 4 步，注册成功后，单击“RMS 全局管理”链接，如图 3-146 所示。返回管理站点，然后单击“在此网站上管理 RMS”链接，返回到 RMS 管理站点。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

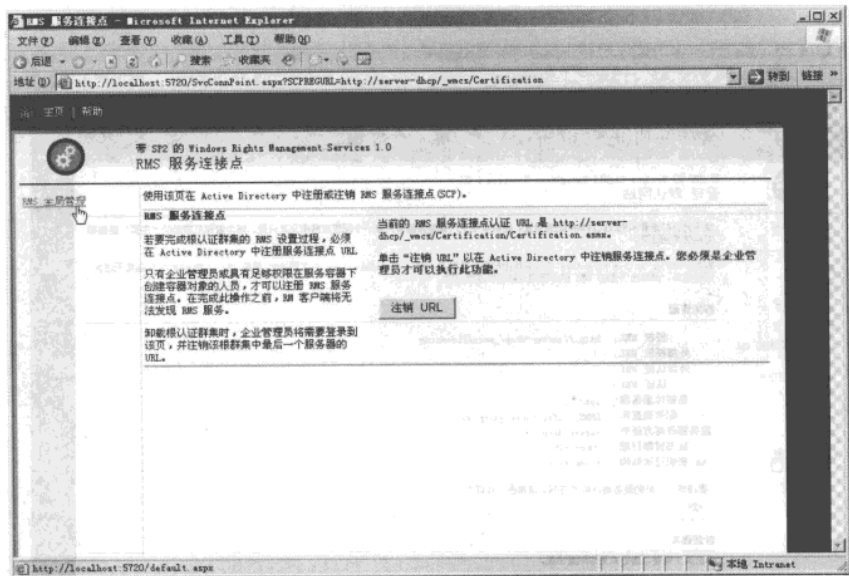


图 3-146 返回 RMS 全局管理

第 5 步，在“RMS 全局管理”页中，单击“Extranet 群集的 URL 设置”链接，在右侧，指定“Extranet 群集的 URL”地址，此地址需要是一个 DNS 名称，并需要解析到 RMS 服务器的 IP 地址，在本例中，此名称为 `rms.heuet.com`，如图 3-147 所示。

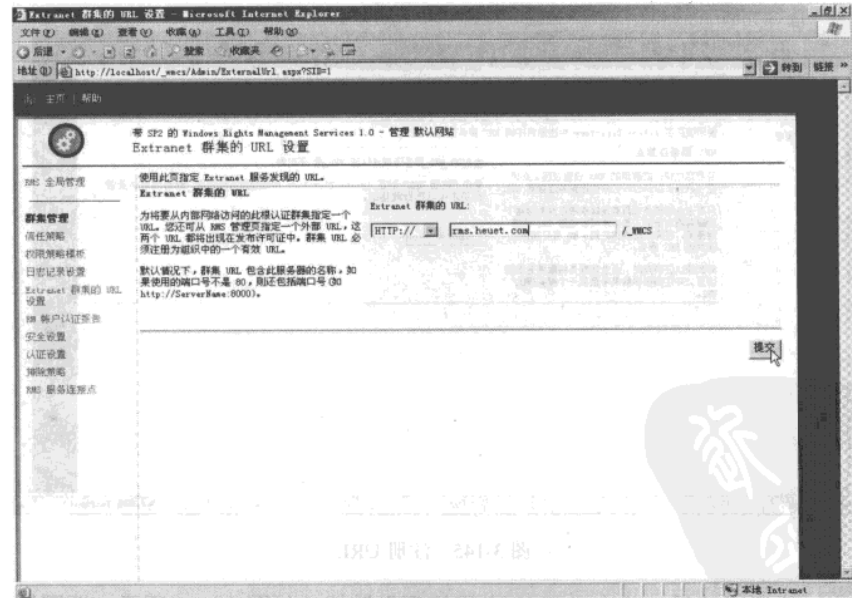


图 3-147 指定外部 URL 地址

说明

在企业网络中，此 DNS 要被解析到 RMS 服务器的地址。如果 RMS 服务器需要在 Internet 上对外提供验证，RMS 服务器通过代理服务器或者防火墙被映射到 Internet 上的一个地址上，则此处填写的 DNS 要被解析到 RMS 服务器所映射的外部公网地址上。

在图 3-147 中设置 URL 后，单击“提交”按钮，会弹出图 3-148 的对话框，单击“确定”按钮。

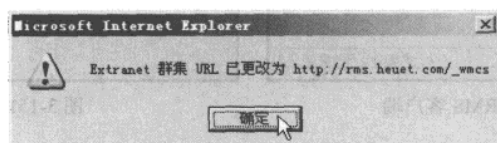


图 3-148 设置 URL 地址成功

关于 RMS 服务器的配置先介绍到此，下面通过具体的例子，介绍 RMS 在企业网络中的应用。

3. 客户端使用

在此以举例的方式，介绍怎样在企业网络中保护 Word 文档。在进行操作之前，请在 Active Directory 服务器中创建几个账户用于测试。在本节实验中，需要创建 zhangsan（张三）、lisi（李四）、wangwu（王五）等三个账户，并且为每个账户创建对应用邮箱，邮箱为用户名@heuet.com。关于这些操作，下面将不再介绍。

在本节内容中，将介绍 RMS 客户端软件的安装、使用 RMS 限制文档的访问等使用方法。

（1）在客户端计算机上安装 RMS 客户端软件。

在网络中的每台工作站上，安装 RMS 的客户端软件及 Office 2003，本节以在“张三”计算机上的安装为例进行说明。

第 1 步，以域用户“张三”的身份登录到计算机，如图 3-149 所示。



图 3-149 登录到域

第 2 步，RMS 的客户端分 64 位版本和 32 位版本，64 位简体中文版安装程序的文件名为“WindowsRightsManagementServicesSP2-KB917275-Client-CHS-X64.exe”，大小为 4894KB；32 位简体中文版安装程序的文件名为“WindowsRights Management ServicesSP2-KB917275-Client-CHS-X86.exe”，大小为 2371KB。请按照你的客户端计算机操作系统的类型，下载并安装对应的版本。RMS 客户端程序的安装比较简单，完全按照默认值，即可以完成安装，如图 3-150 和图 3-151 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

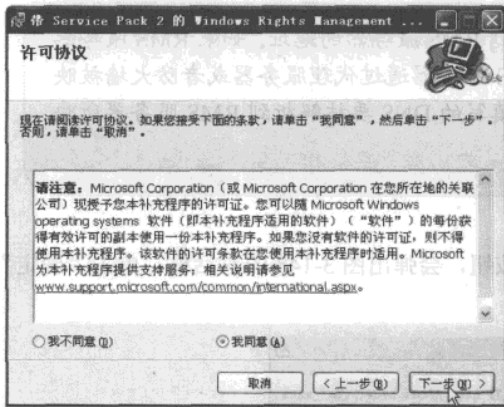


图 3-150 安装 RMS 客户端

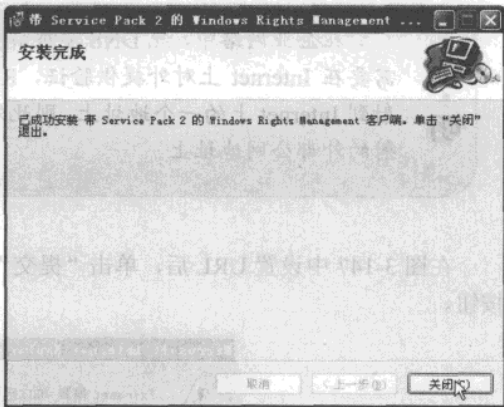


图 3-151 安装完成

(2) 使用 RMS 签发文档。

在安装 RMS 客户端后，就可以在 Office 中打开或创建带安全保护的文档了，下面将在“张三”的计算机上，创建一个文档，此文档可以让李四更改、让王五只读并不能复制、打印其内容，并且此文档在 1 个月过后过期，下面来看操作步骤。

第 1 步，使用域用户“张三”的用户名登录到计算机，打开 Word 文档，编辑一篇文档。文档编辑完成后，打开“文件”菜单，选择“权限”→“限制权限为”命令，如图 3-152 所示。

第 2 步，如果是第一次使用该功能，会弹出如图 3-153 所示的对话框。

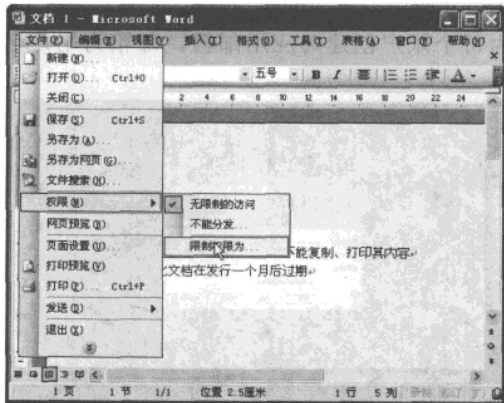


图 3-152 限制文档权限

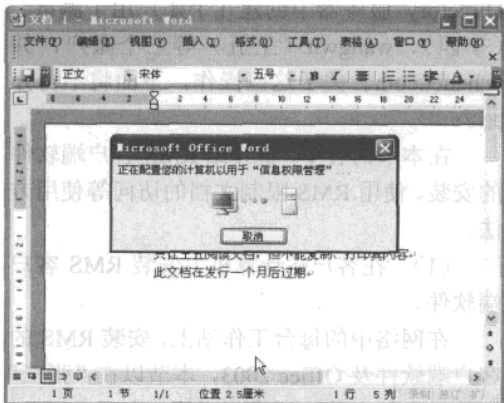


图 3-153 第一次使用时要配置计算机用于 RMS

第 3 步，在弹出的“选择用户”对话框中，选中“始终使用此账户”复选框，然后单击“确定”按钮，如图 3-154 所示。

说明

图 3-154 中的账户，就是当前用户“张三”的邮箱，如果该用户使用其他邮箱，请单击“添加”按钮，添加其他的管理邮箱。

服务器方面 | 3

第 4 步，在“权限”对话框中，选中“限制对此文档的权限”复选框，在“读取”文本框中，输入允许读取当前文档的用户的邮箱。在本例中输入 wangwu@heuet.com；在“更改”文本框中，输入允许更改当前文档的用户的邮箱，在本例中输入 lisi@heuet.com。然后单击“其他选项”按钮，进入高级权限设置页，如图 3-155 所示。

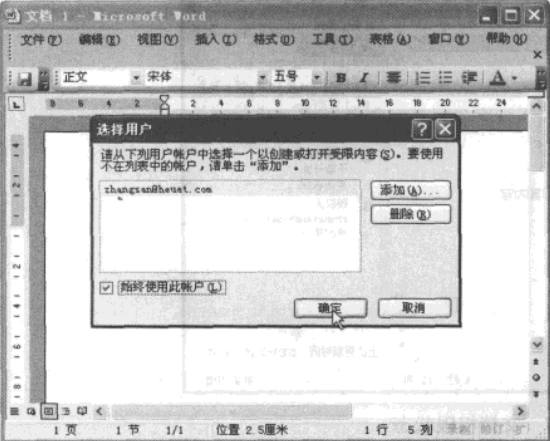


图 3-154 添加管理账户

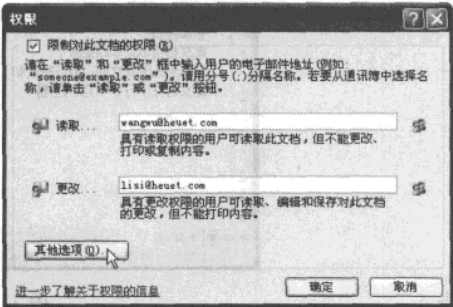


图 3-155 添加用户

第 5 步，在弹出的“权限”对话框中，选中“此文档的到期日期为”复选框，并且输入当前文档的到期时间，如果允许用户打开，则选中“打印内容”复选框；如果允许用户通过“粘贴”、“复制”以复制此文档内容，请选中“允许具有读取权限的用户复制内容”复选框；如果选中“要求连线验证用户权限”复选框，则其他用户读取此文档时，需要从 RMS 服务器上验证其权限。在“用户可以从此处请求附加权限”文本框中，默认为文档所有人的邮箱。这样，当其他用户不能访问被限制的文档时，可以发邮件到文档所有人邮箱，由所有人更改文档的权限。

以上信息，请根据需要进行配置，如图 3-156 所示。

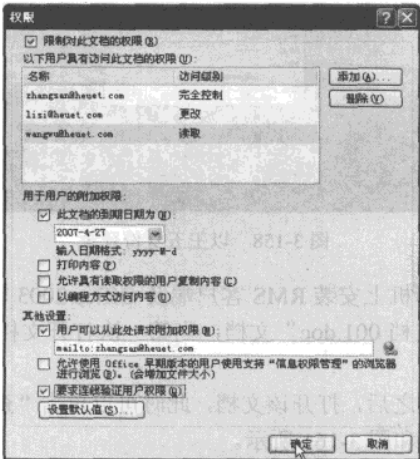


图 3-156 权限设置页

网管天下 网管经验谈

在图 3-156 中，还可以单击“添加”、“删除”按钮，添加或删除用户。

第 6 步，设置权限后，在“共享工作区”中将显示文档的状态，如图 3-157 所示。

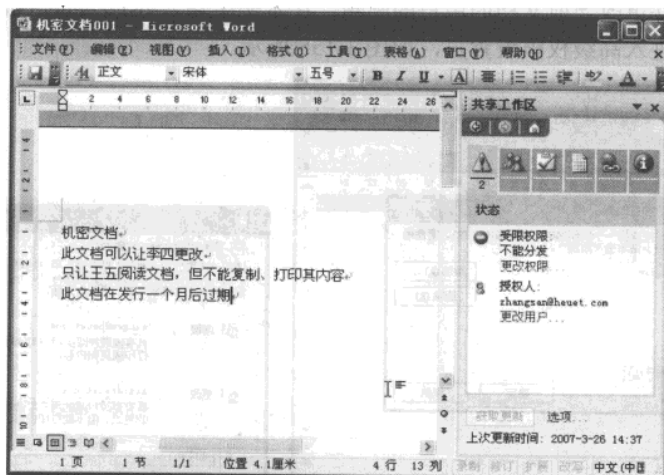


图 3-157 文档权限状态

第 7 步，将此文档保存为“机密文档 001.doc”，然后发送给“李四”和“王五”，让其验证 RMS 权限设置。

(3) 验证分发的文档。

首先来到“王五”的计算机上，安装 RMS 客户端及 Office 2003 程序，验证图 3-157 中保存的文档（可以用各种方式将此文档复制到王五的计算机上），主要步骤如下。

第 1 步，以域用户“王五”的用户名登录计算机，如图 3-158 所示。

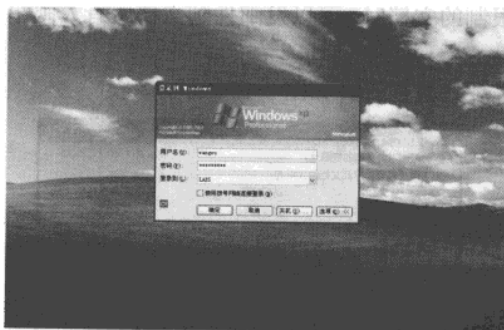


图 3-158 以王五身份登录

第 2 步，在当前的计算机上安装 RMS 客户端及 Office 2003 软件。

第 3 步，打开“机房文档 001.doc”文档，当第一次打开文档时，会提示用户进行在线验证工作，如图 3-159 所示。

第 4 步，在线验证通过之后，打开该文档，此时可以单击“查看我的权限”链接，查看当前用户的权限，如图 3-160 和图 3-161 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

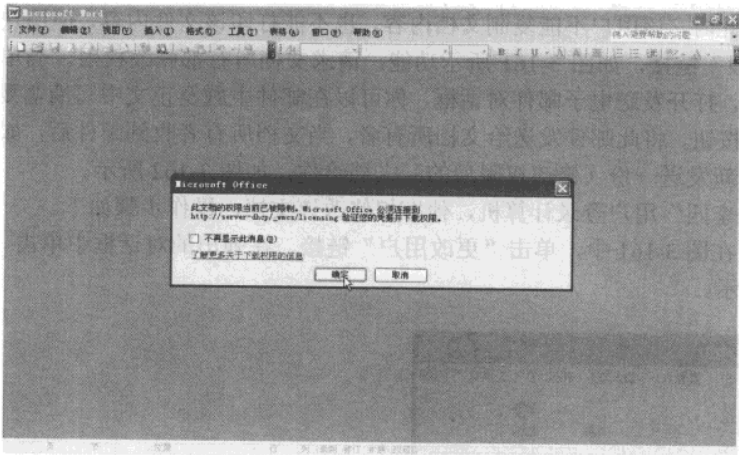


图 3-159 在线验证

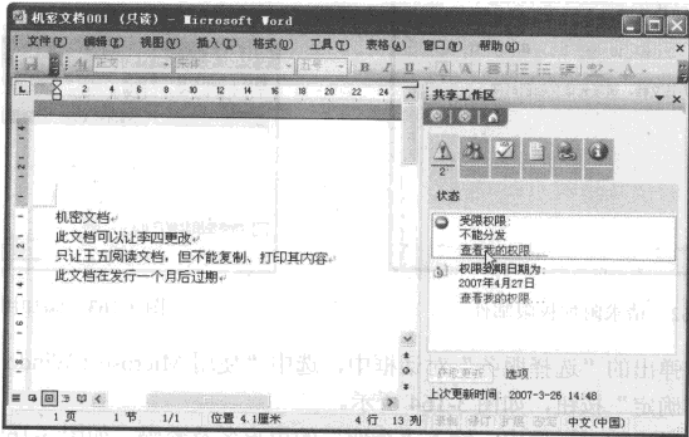


图 3-160 查看我的权限

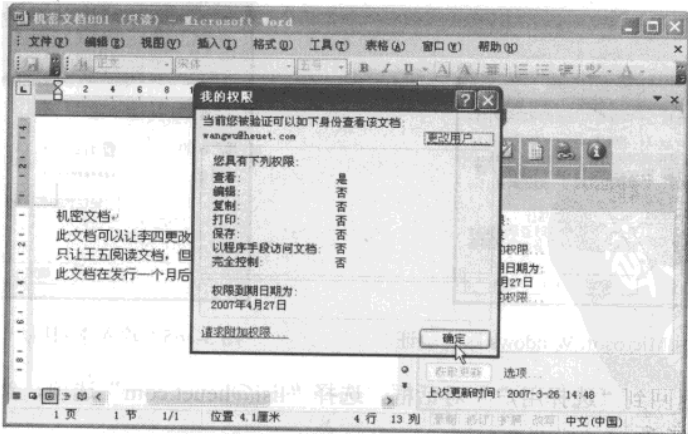


图 3-161 列表当前用户的权限

网管天下 网管经验谈

第 5 步，此时，该用户不能复制文档内容，也不能打印该文件内容，但用户可以通过单击“请求附加权限”链接，如图 3-161 所示功能，请求文档所有都修改权限。当单击“请求附加权限”链接时，打开发送电子邮件对话框，你可以在邮件主题及正文中写清需要的权限，然后单击“发送”按钮，将此邮件发送给文档所有者，当文档所有者收到邮件后，如果批准你的权限，他将会重新发送一份（修改权限后的）文档给你，如图 3-162 所示。

如果以“李四”用户登录计算机，他有权修改该文档，操作步骤如下。

第 1 步，在图 3-161 中，单击“更改用户”链接，在弹出的对话框中单击“添加”按钮，如图 3-163 所示。

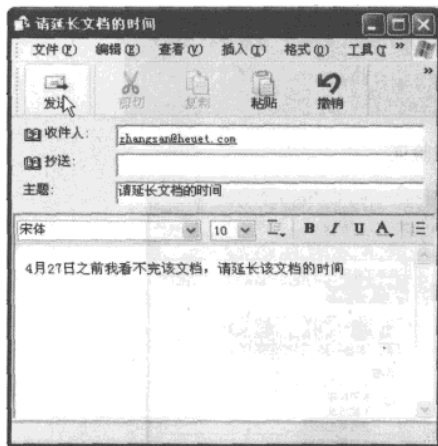


图 3-162 请求附加权限邮件

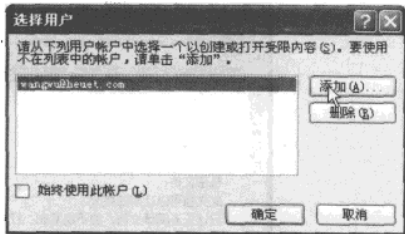


图 3-163 添加用户

第 2 步，在弹出的“选择服务”对话框中，选中“使用 Microsoft Windows 账户”单选按钮，然后单击“确定”按钮，如图 3-164 所示。

第 3 步，在弹出的对话框中，输入“李四”的用户名及密码，如图 3-165 所示。

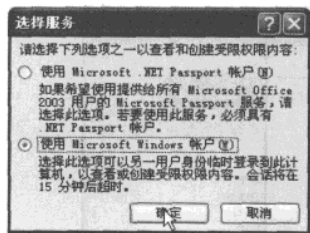


图 3-164 使用 Microsoft Windows 账户验证

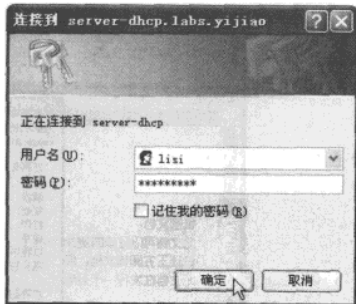


图 3-165 输入李四用户名进行验证

第 4 步，返回到“选择用户”对话框，选择“lisi@heuet.com”选项，然后单击“确定”按钮，如图 3-166 所示。

第 5 步，再次打开文档后，查看用户权限，如图 3-167 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

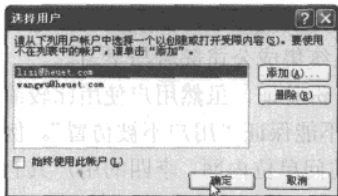


图 3-166 选择使用李四用户

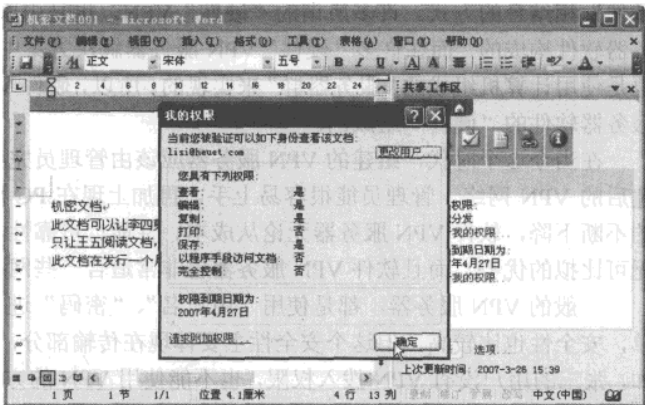


图 3-167 该文档可以被复制、编辑、打印

说·明 在本次操作中，你也可以不按照图 3-162 ~ 图 3-167 的操作，而是直接返回到李四的计算机上，以李四用户名密码登录后再查看文档，与图 3-167 效果一致。本次演示表明，当你有多个用户身份时，可以不必注销计算机，而直接以另一个身份登录并获得相应的权限。

3.5 轻松管理服务器的经验

管理服务器是网管员日常维护和管理的最基本的工作之一。如何轻松地实现对服务器的管理呢？本文介绍了几个常见的管理经验，为读者管理网络提供参考。

3.5.1 轻松实现智能化身份验证

传统的 VPN 服务器大多采用“硬件”方式，但这种方式存在以下的缺点：

- (1) 使用的 VPN 服务器有容量限制，例如，有的用户初期购买 60 个并发连接的 VPN 设备，当用户的需求超过 60 个时，只能丢掉原来的设备，购买更大容量的 VPN 接入设备，造成用户原有投资的浪费。
- (2) 硬件 VPN 组网简单、配置固定。一般硬件 VPN 只有两个或者 3 个接口，只适合一般的企业，如果企业对网络有更复杂或者更灵活的要求，一般的硬件 VPN 都不能满足。
- (3) 兼容性差。一般硬件 VPN 采用自己的标准或者协议，没有采用工业标准，如果企业在组建 VPN 网络时，或者所有的设备都采用同一厂家的设备，否则容易造成互连互通的问题。
- (4) 维护困难。一般的硬件 VPN，因为各种原因，只能由自己公司的技术人员调试。当用户使用一般时间，想对 VPN 网络进行进一步的定制或者改造时，只能求助于厂家的技术人员。
- (5) 传统的 VPN 组网，不适合由网管员自己组建，也不适合网管员管理。而本文将介绍采用“软件”VPN 方式组网。实际上，所谓“软件”VPN 也好，“硬件”VPN 也罢，都是“软、

网管天下 网管经验谈

硬件”相结合的方式。许多所谓的“硬件”VPN，也是由服务器、硬盘、操作系统、VPN 服务器软件构成的，而在许多“硬件”VPN 服务器解决方案中，在超过 10 000 万个并发连接时，也是使用计算机组成的“服务器群”来实现的。所以，硬件 VPN 服务器，最终也是由运行 VPN 服务器软件的“硬件”组成的。

在当今这个时代，组建的 VPN 服务器应该由管理员完全控制或者“一手”组建，或者组建后的 VPN 网络，管理员能很容易上手，再加上现在 PC 服务器硬件性能的不提高与成本的不断下降，软件 VPN 服务器无论从成本、性能、可靠性，还是安全性、可扩展性上，都有无可比拟的优势，而且软件 VPN 服务器也非常适合一些网络系统集成公司部署与学习。

一般的 VPN 服务器，都是使用“用户名”、“密码”进行身份验证，虽然用户使用比较简单，安全性也比较高，但这个安全性主要体现在传输部分，它不能保证“用户不被仿冒”。例如，张三的用户没有 VPN 拨入权限，也不能使用 VPN 的方式访问单位内网，李四的用户具有 VPN 拨入权限。假设张三知道了李四的密码，张三就可以使用李四的用户名和密码拨叫 VPN 服务器并访问内网。李四为了避免张三（或者其他用户）知道自己的用户名密码，就要经常修改密码，并且要设置非常复杂的密码，例如，2@#Ui)8 这个密码，被认为是复杂密码，但这样一来，李四就不容易记住自己的密码。另外，有许多时候，张三和李四认识，张三可能会打电话询问李四 VPN 的账户和密码，李四耐于情面也会告诉张三 VPN 的账户和密码。

为了避免这个问题，可以使用“智能卡”的方式进行验证。使用智能卡后，将会改进传统的以用户名、密码进行验证的方式。当用户需要拨叫 VPN 服务器时，必须插入智能卡，由 VPN 拨号程序访问智能卡，通过读取智能卡中保存的信息进行身体验证。这样就可以达到只让指定的用户访问 VPN 服务器的目的。而本节要给大家介绍的正是这方面的内容。

说明

从 Windows 2000 Server 开始就支持智能卡，但必须以 Active Directory 为基础，所以组建使用智能卡进行身份验证的 VPN 服务器需要“域服务器”的支持。使用智能卡进行身份验证，实际上是使用保存在智能卡中的证书进行验证，所以还需要“证书服务器”，而只有 Windows Server 中的“企业证书服务器”才能与 Active Directory 进行集成，所以，使用智能卡的 VPN 网络，还需要“企业证书服务器”的支持。

1. 使用智能卡验证的 VPN 网络拓扑结构

在商用的 VPN 服务器中，包括一些“硬件”VPN 服务器，大多采用“智能卡”作为身份验证的工具，一是可以提高 VPN 系统的安全性，另外可以提升产品的价值。但实际上，智能卡与常用的计算机（文本）证书、用户名、密码一样，只是身份验证的一种方法，不过由于智能卡不容易仿冒，所以安全性相对来说较高而已。如果用户名、密码设置得非常复杂，例如使用 Ae\$7Y 之类的用户名、采用 U*7%\$E0@d8 之类的密码，其安全性也是非常高的。只不过使用如此复杂的密码，会产生不易记忆的问题，而采用智能卡就可以解决这些问题。

使用智能卡具有以下 4 条优点：

- （1） 用户不再需要记住复杂的密码。用户只需要记住智能卡的“PIN”码就可以使用智能卡，PIN 码可以非常简单，例如可以用 123、5678、abc 或者其他容易记住的密码即可。
- （2） 和银行的存折、信用卡一样，智能卡需要由“认证中心（即企业证书服务器）”统

一颁发、续订，用户的智能卡丢失后，可以申请挂失。如果用户的智能卡丢失，拾到智能卡的用户如果尝试使用智能卡，在输入错误的 PIN 码达到次数后（例如 3 次），智能卡将被锁定。

(3) 智能卡具有“唯一性”，可以为需要的用户颁发智能卡。

(4) 安全性高：智能卡采用硬件加密，安全可靠。

说
明

一般学校食堂使用的饭卡、银行发行的信用卡，包括网上银行使用的“U 盾”等都是智能卡。从 Windows 2000 开始，操作系统就已经支持“智能卡”，使用本书介绍的智能卡，除了可以作 VPN 用户的身份验证外，还可以用“智能卡”代替用户输入用户名与密码。也就是说，当用户登录计算机时，可以不需要输入用户名与密码，只需插入智能卡并输入智能卡的 PIN 码（通常是比较简单的）就可以登录计算机，当拔下智能卡时，计算机将被锁定。而在 Windows Server 2003、Windows Server 2008、Windows XP 中，还可以用智能卡登录远程的 Windows Server 2003、Windows Server 2008 的终端服务器。

本节采用图 3-168 所示的网络拓扑进行介绍。

在图 3-168 中，使用智能卡进行验证的 VPN 网络需要“VPN 服务器、Windows Server 2003 的 Active Directory 服务器、企业证书服务器”，其中 Active Directory 服务器是基础，企业证书服务器与 VPN 服务器都要加入 Active Directory，而使用智能卡进行身份验证的 VPN 客户端，不需要加入 Active Directory。

在图 3-168 中做如下的设定：Windows Server 2003 的 Active Directory 服务器的域名是 msft.com，IP 地址是 172.30.5.3/24，企业证书服务器的 IP 地址是 172.30.5.4，VPN 服务器的内网地址是 172.30.5.5，外网地址是 202.206.197.101。其中 Active Directory 服务器与企业证书服务器都只需要一块网卡，VPN 服务器需要两块网卡。

采用智能卡进行身份验证的 VPN 网络组建的主要步骤如下：

第 1 步，在将要做 Active Directory 服务器的计算机上，安装 Windows Server 2003，设置 IP 地址与 DNS 地址（在本节中都是 172.30.5.3）。

第 2 步，在将要做证书服务器的计算机上，设置 IP 地址（172.30.5.4）与 DNS 地址（172.30.5.3），加入到 Active Directory 中作“成员服务器”，并安装证书服务。在实际使用中，“企业证书服务器”可以与“Active Directory”在同一台计算机上。

第 3 步，在将要做 VPN 服务器的计算机上，设置内、外网 IP 地址并分别设置 DNS 服务器，并加入“Active Directory”做“成员服务器”，然后安装 ISA Server 并创建策略。

第 4 步，在“企业证书服务器”上，安装智能卡驱动程序，并配置“证书颁发机构”。

第 5 步，在企业证书服务器上（或者管理工作站上），安装智能卡驱动程序，以域管理员身份登录，一一插入智能卡，并将验证信息写入智能卡。

第 6 步，在 VPN 客户端计算机上，安装智能卡驱动程序、信任企业证书颁发机构、创建 VPN 客户端连接，之后使用智能卡进行验证拨叫 VPN 服务器。

为了方便详细讲解，把图 3-168 简化成图 3-169，每个服务器的名称、IP 地址与配置的顺序如表 3-4 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

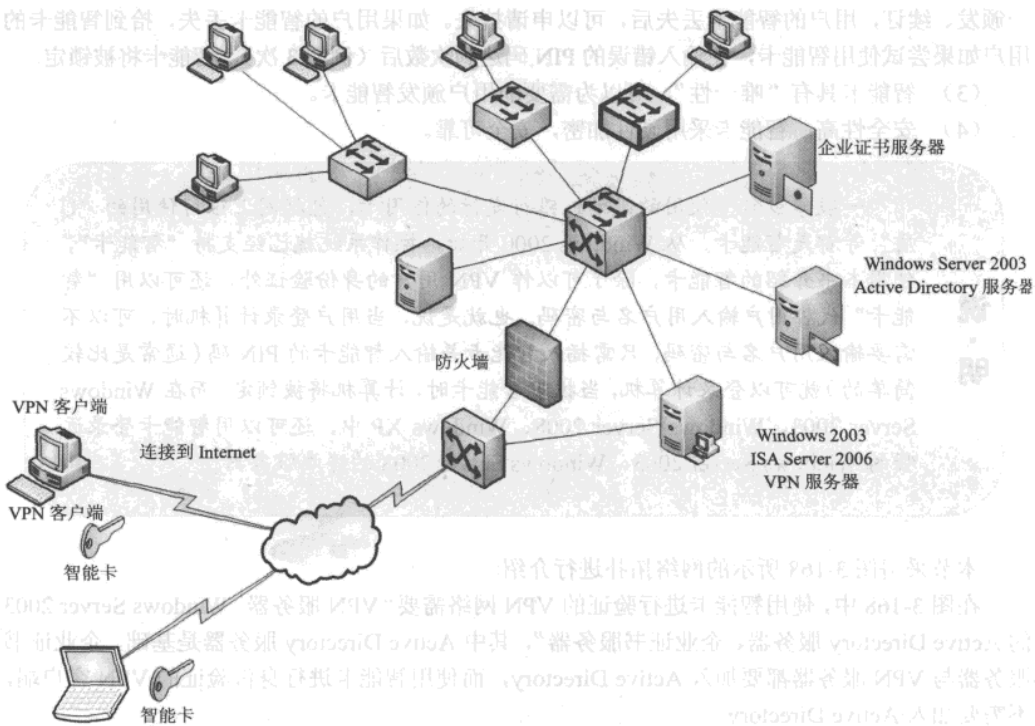


图 3-168 使用智能卡进行身份验证的 VPN 网络拓扑



图 3-169 简化的智能卡 VPN 网络拓扑

表 3-4 IP 地址与配置情况

顺 序	计 算 机 名	IP 地址/24	DNS 地址	DNS 域名	描 述
1	AD-SERVER	172.30.5.3	172.30.5.3	MSFT.COM	域控制器、证书服务器
2	VPN-Server	172.30.5.5	172.30.5.3	MSFT.COM	内网网卡
		202.206.197.101			外网网卡
3	XP	202.206.197.102			VPN 客户端

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意 不要用 VPN 服务器做 Active Directory 服务器，VPN 服务器与 Active Directory 应该分开，但可以将“证书服务器”与“Active Directory”放在同一台服务器上。

2. 准备 Windows Server 2003 的 Active Directory 服务器

在将要安装 Active Directory 服务器的计算机上，安装 Windows Server 2003 的标准版或者企业版，修改计算机名称、设置 IP 地址并升级到 Active Directory，主要步骤如下。

第 1 步，修改计算机名称为 ad-server，并重新启动计算机。

第 2 步，设置 IP 地址为 172.30.5.3，子网掩码为 255.255.255.0，设置 DNS 为 127.0.0.1（代表本机地址，也可以设置为 172.30.5.3）。

说明 在实际使用中，必须要根据实际情况设置网关地址。

第 3 步，接下来要将计算机升级到“Active Directory（活动目录）”。在升级的过程中，指定域名为“msft.com”，如图 3-170 所示。

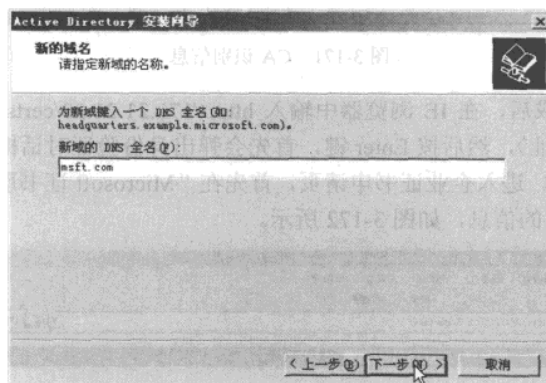


图 3-170 指定域名

第 4 步，安装完成后，单击“立即重新启动”按钮，重新启动 Windows Server 2003 的计算机，完成 Active Directory 的安装。

3. 准备企业证书服务器

使用智能卡进行身份验证的 VPN 网络中，企业证书服务器是必须的选择，不能使用“标准证书服务器”，可以将企业证书服务器与 Active Directory 服务器共同安装在同一台服务器上。企业证书服务器的安装比较简单，下面只介绍其主要步骤。

第 1 步，在 Active Directory 服务器上，以管理员身份登录，在“控制面板”→“添加/删

网管天下 网管经验谈

除程序”→“添加/删除 Windows 组件”中，先安装（选中）“应用程序服务器→ASP.NET 和 Internet 信息服务”。

第 2 步，然后安装证书服务，单击“下一步”按钮，在“CA 类型”页中，选择“企业根 CA”。

第 3 步，在“CA 识别信息”页中的“此 CA 的公用名称”文本框中，输入该企业根 CA 的信息，例如 ent-ca.msft.com，这个信息将在用 IE 申请证书时出现在证书申请首页中，并且，最好将这个名称注册为 DNS 域名对外提供服务，在“有效期限”页中，选择该证书服务器的有限期限，默认为 5 年，如图 3-171 所示。

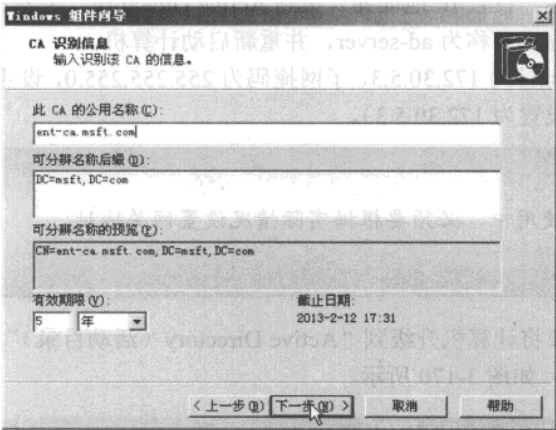


图 3-171 CA 识别信息

第 4 步，安装完成后，在 IE 浏览器中输入 http://172.21.21.23/certsrv（其中 172.21.21.23 是证书服务器的 IP 地址），然后按 Enter 键，首先会弹出身份验证对话框，输入管理员账户和密码，接着按 Enter 键，进入企业证书申请页，首先在“Microsoft 证书服务器”后面显示的名称就是图 3-171 中输入的信息，如图 3-172 所示。

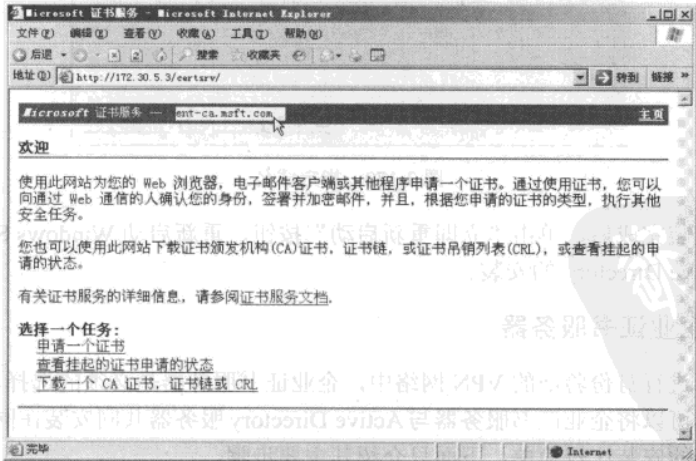


图 3-172 企业证书申请页

4. 准备 VPN 服务器

在准备做 VPN 服务器的计算机上，需要经过一系列步骤的配置，才可以让 VPN 服务器使用智能卡进行身份验证，这些步骤主要有：

(1) VPN 服务器基本准备。

在准备做 VPN 服务器的计算机上，首先设置内网网卡的 IP 地址为 172.30.5.5，设置 DNS 地址为 172.30.5.3，设置外网网卡的 IP 地址为 202.206.197.101，设置网关地址为 202.206.197.4，并且将内网网卡重命名为“LAN”，将外网网卡重命名为“Internet”。然后重命名计算机为 VPN-Server，之后重新启动计算机。最后，确认该计算机没有安装 IIS、没有启用 Windows 内置的防火墙与没有启用“路由和远程访问”服务。

(2) 将计算机加入到 Active Directory。

接下来将计算机加入到 Active Directory，作为域 msft.com 的成员服务器，其具体步骤在此不做过多介绍。

(3) 安装 ISA Server。

以域管理员的身份登录到域，然后开始安装 ISA Server 2006，需要注意：

- ① 不要安装“高级日志”。
- ② 选择“内网”网卡为内部网络，如图 3-173 所示。

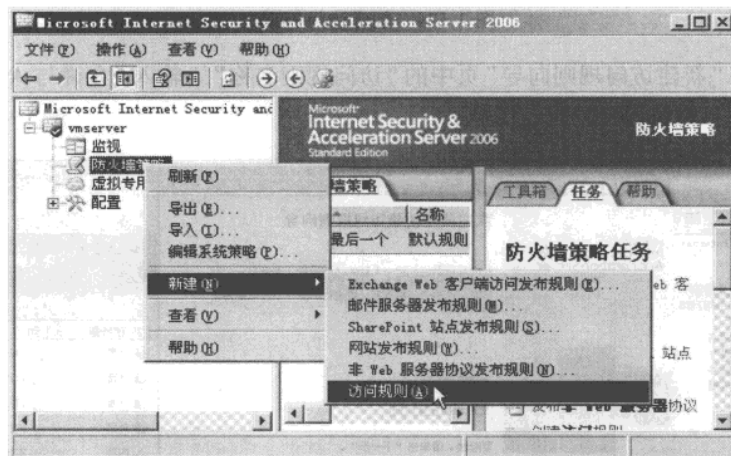


图 3-173 选择内部网络

(4) 其他均采用默认安装即可，这里不再多做介绍。

5. 申请证书

在配置 VPN 服务器之前，需要为该服务器申请一个“计算机证书”，但因为这台计算机安装了 ISA Server，默认是阻止这台计算机访问其他服务器的，所以需要创建访问策略。

打开 ISA Server 服务器，创建一条策略，该策略允许 Active Directory 服务器（IP 地址为 172.30.5.3）的计算机与 ISA Server 服务器（即 VPN 服务器）可以以任意协议“互相”通信，创建该策略主要步骤如下。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 1 步，在 ISA Server 管理控制台，新建访问规则，如图 3-174 所示。

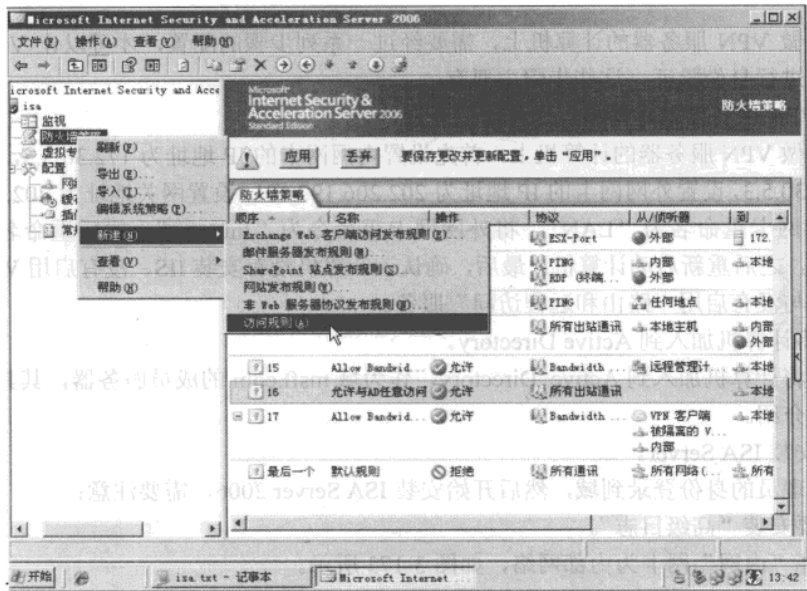


图 3-174 创建访问规则

第 2 步，在“新建访问规则向导”页中的“访问规则名称”下输入“允许与 AD 任意访问”，如图 3-175 所示，单击“下一步”按钮。

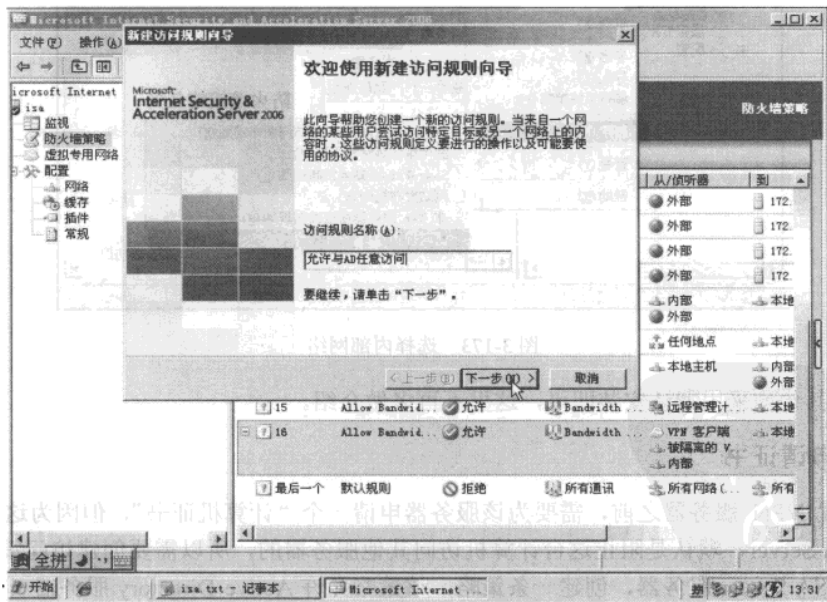


图 3-175 访问规则名称

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

第 3 步，在“新建访问规则向导”页中的“在符合规则条件时要执行的操作”下选中“允许”单选按钮，如图 3-176 所示。

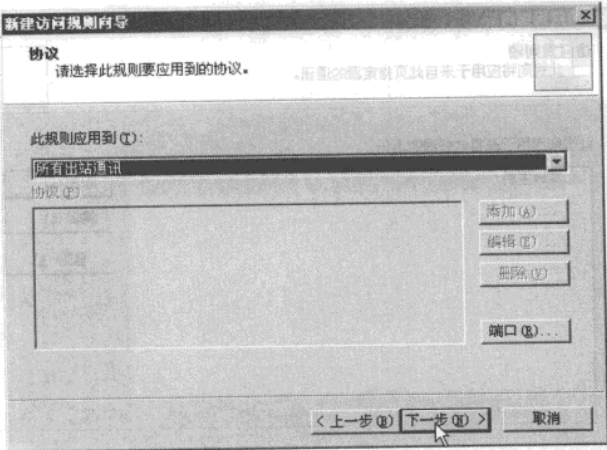


图 3-176 允许操作

第 4 步，在“新建访问规则向导”页中的“此规则应用到”下拉列表框中选择“所有出站通讯”选项，如图 3-177 所示。

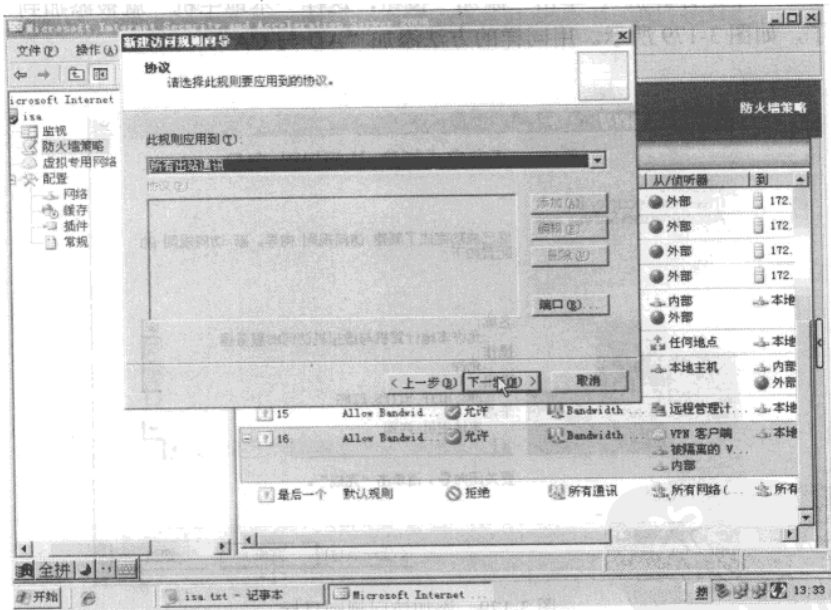


图 3-177 访问规则协议

第 5 步，在“访问规则源”页中单击“添加”按钮，在“添加网络实体”对话框中选择“新建→计算机集”，在“新建计算机集规则元素”对话框中的“名称”文本框后面输入“AD 与 CA”，然后单击“添加→计算机”，在弹出的对话框中输入 Active Directory 服务器的计算机

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

的 IP 地址，然后单击“确定”按钮。添加完成后，将“本地主机”与新添加的“AD 与 CA”添加到“访问规则源”页中，如图 3-178 所示。

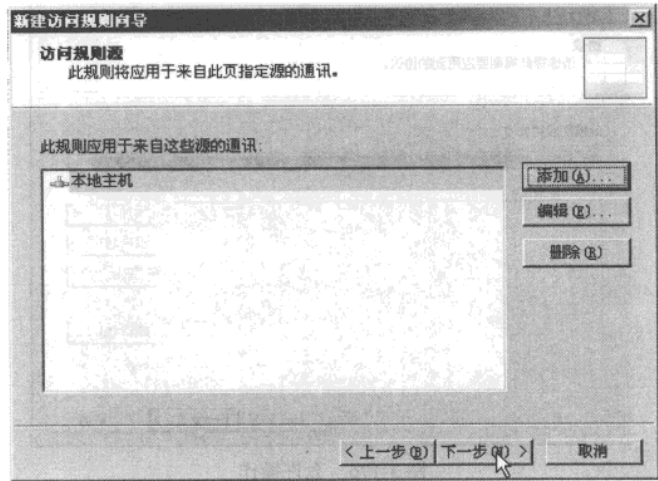


图 3-178 添加访问规则源

第 6 步，在“访问规则目标”页中，单击“添加”按钮，在弹出的“添加网络实体”中选择“网络——本地计算机”，单击“添加”按钮，这样“本地主机”就被添加到“访问规则目标”中了，如图 3-179 所示。用同样的方法添加“AD 与 CA”。

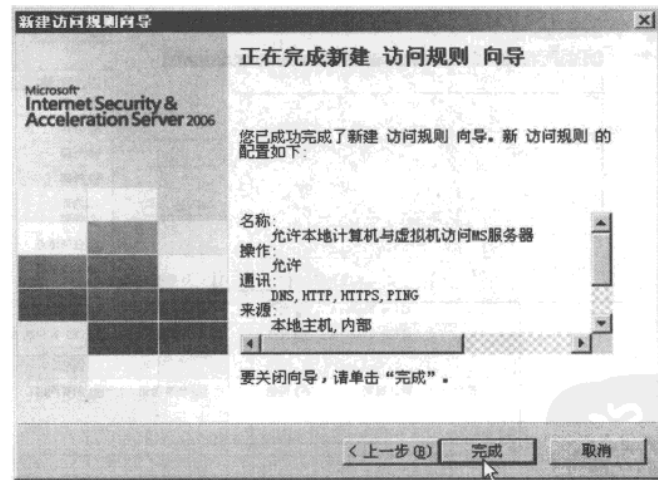


图 3-179 添加访问规则目标

第 7 步，其他选择默认值，设置完成后单击“完成”按钮，如图 3-180 所示。在完成设置后即生效。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 3

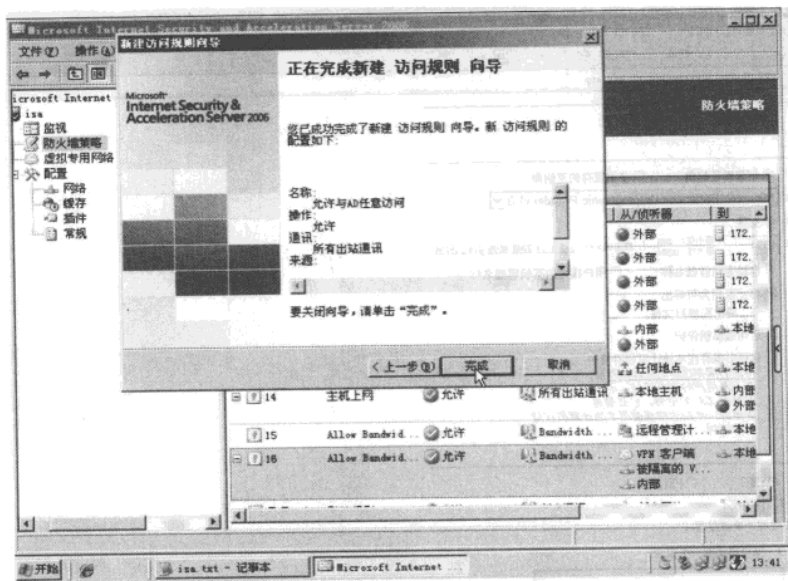


图 3-180 完成创建规则

在创建访问规则之后，就可以为 VPN 服务器从“企业证书服务器”申请“计算机证书”，主要步骤如下：

第 1 步，在 VPN 服务器计算机上，打开 IE 浏览器，输入 <http://172.21.21.23/certsrv/>，在弹出的对话框中输入域管理员账户和密码，进入“申请证书”页，如图 3-181 所示。

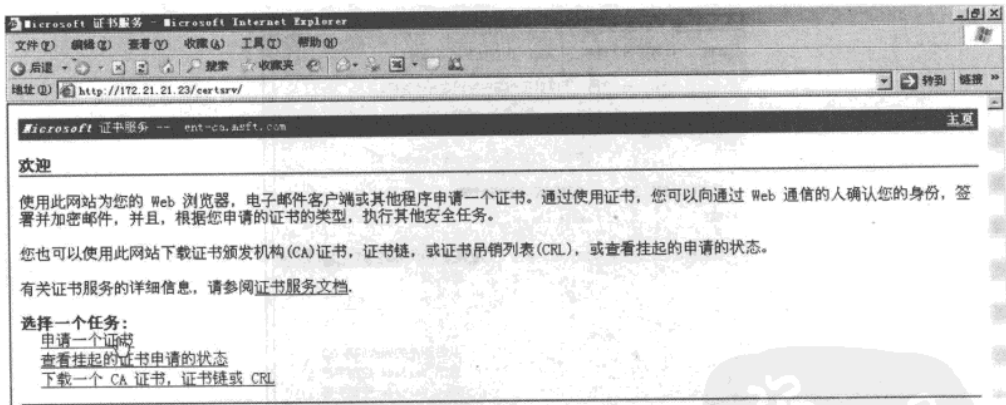


图 3-181 申请证书页

第 2 步，在“欢迎”页中单击“申请一个证书”链接；在“申请一个证书”页中单击“高级证书申请”链接；在“高级证书申请”页中单击“创建并向此 CA 提交一个申请”链接，进入“创建并向 CA 提交申请”页，如图 3-182 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

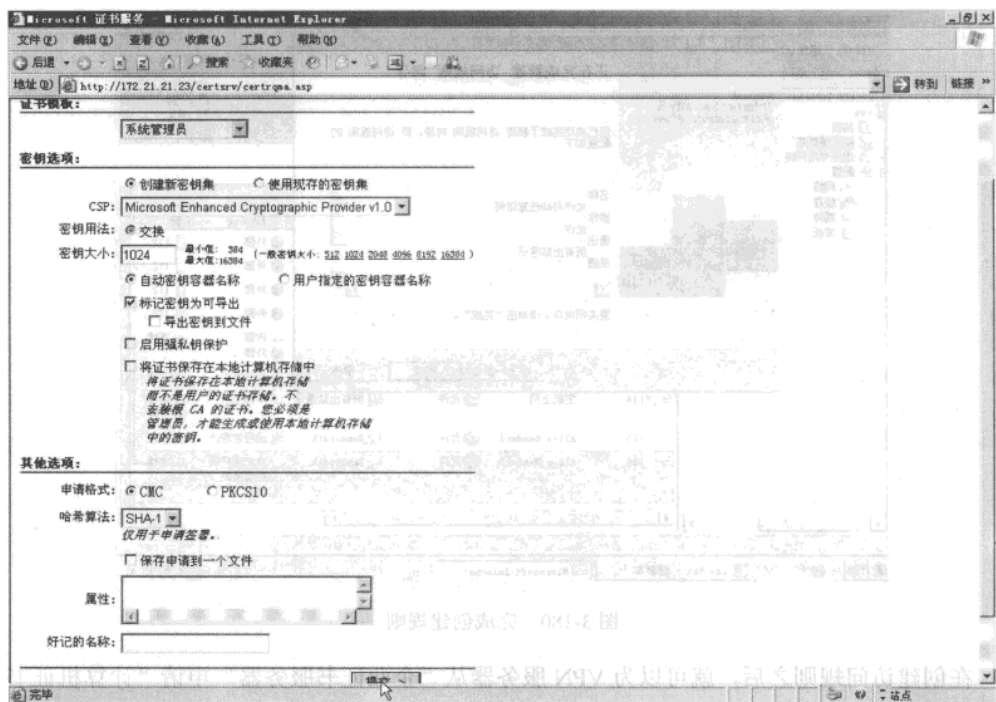


图 3-182 高级创建证书页

第 3 步，然后打开“系统属性”对话框，查看并复制计算机名称，如图 3-183 所示。

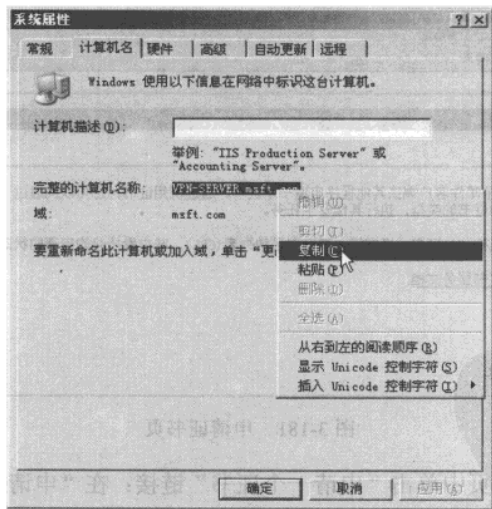


图 3-183 复制计算机名称

第 4 步，切换到“高级证书申请”页，在“高级证书申请”页中的“证书模板”下拉列表框中选择“Web 服务器”，在“姓名”文本框中“粘贴”从图 3-183 中复制的计算机名称，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 3-184 所示。选中“将证书保存在本地计算机存储中”复选框，然后单击“提交”按钮。

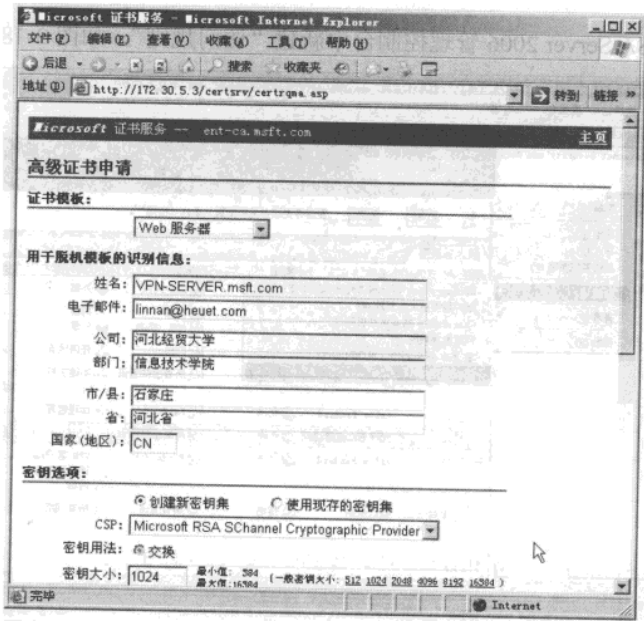


图 3-184 输入正确的计算机名称

第 5 步，从企业证书服务器申请证书时，证书会立刻颁发。在“证书已颁发”页中单击“安装此证书”链接，在弹出的“潜在脚本冲突”中单击“是”按钮，如图 3-185 所示。

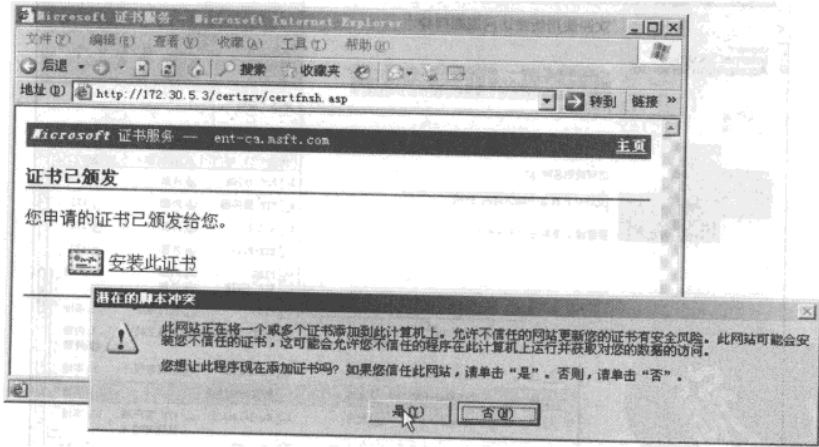


图 3-185 安装已颁发的证书

6. 启用 VPN 服务

在申请并安装证书之后，就可以在 ISA Server 中启用 VPN 服务器了，主要步骤包括：

- (1) 为 VPN 客户端创建访问规则。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

在本节示例中，将允许 VPN 客户端访问“内网”与“外部”，在 ISA Server 中创建的访问规则如下。

第 1 步，在 ISA Server 2006 管理控制台中新建“访问规则”，如图 3-186 所示。

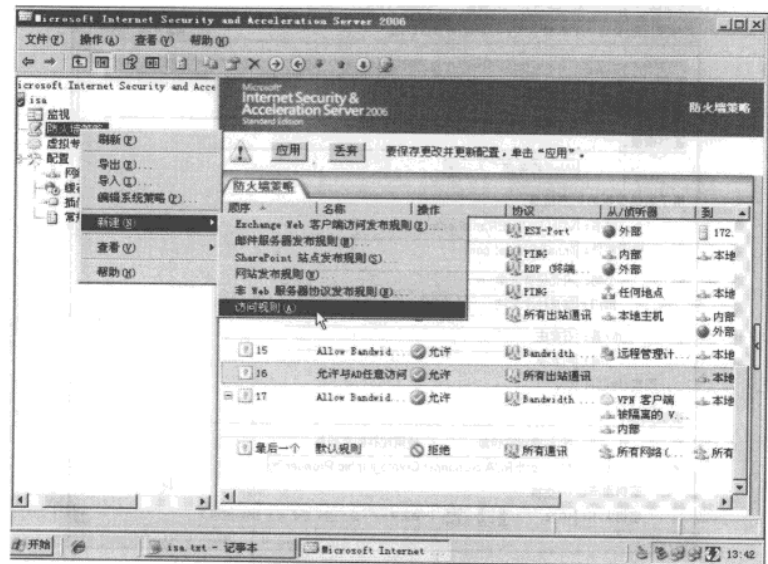


图 3-186 新建访问规则

第 2 步，设置访问规则名称为“允许 VPN 客户端访问内、外网”如图 3-187 所示。

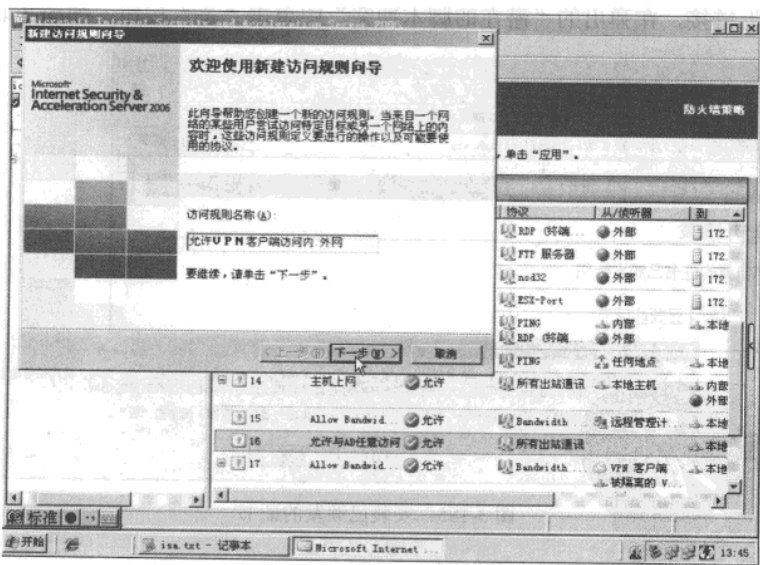


图 3-187 设置访问规则名称

第 3 步，设置访问规则操作为“允许”，再设置“协议”为“所有出站通信”如图 3-188 所示。“访问规则源”中选择“VPN 客户端”，如图 3-189 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

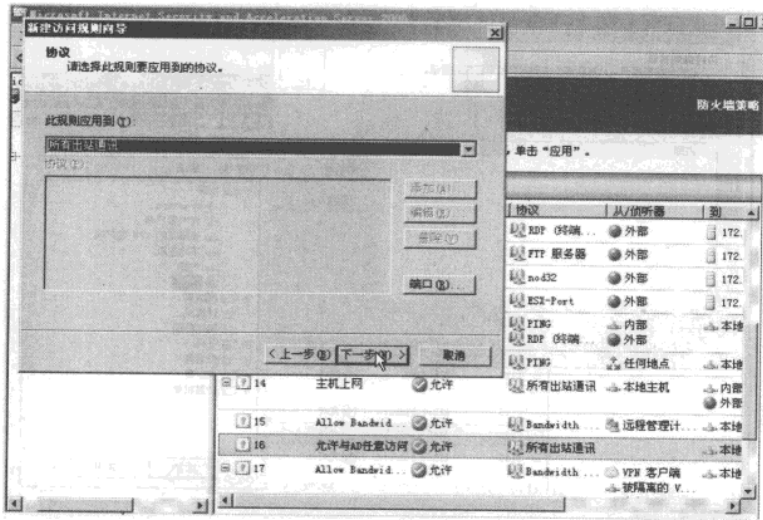


图 3-188 设置协议

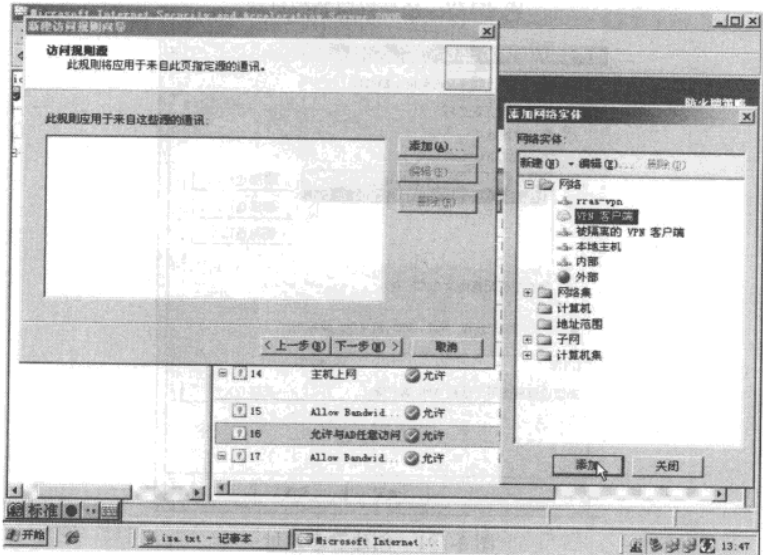


图 3-189 访问规则源

第 4 步，访问规则目标为“内部”、“外部”，如图 3-190 所示。

第 5 步，其他选择默认值即可。

(2) 为使用智能卡验证启用 VPN 服务器。

定位到“虚拟专用网络 (VPN)”，在右侧单击“定义地址分配”链接。

第 1 步，在“地址分配”选项卡中，为 VPN 客户端添加“172.16.100.1~172.16.100.254”的地址，如图 3-191 所示。

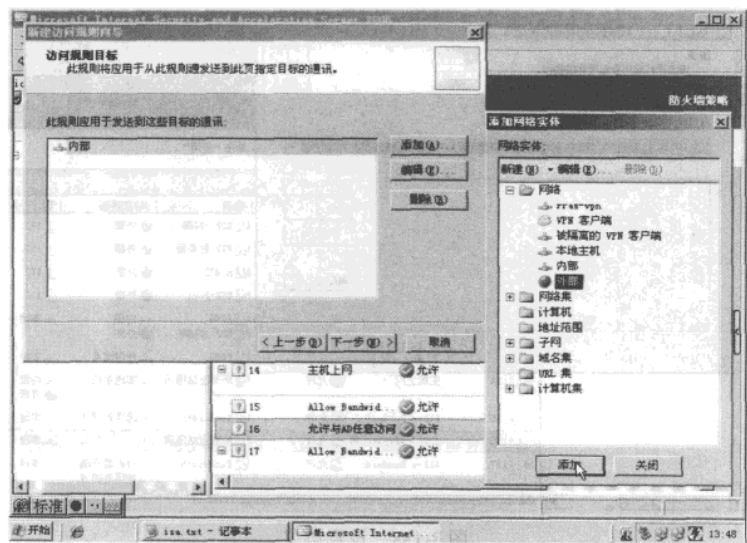


图 3-190 设置访问规则目标

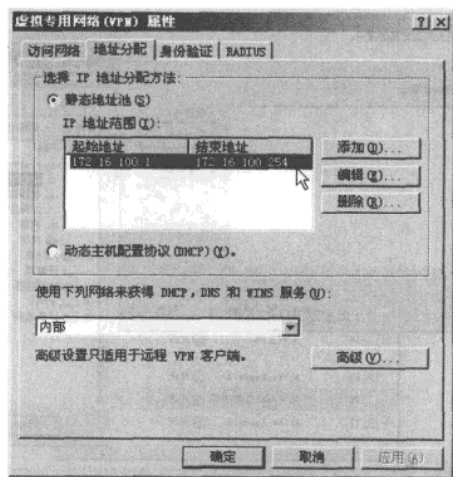


图 3-191 创建静态地址

第 2 步，打开“身份验证”选项卡，取消“Microsoft 加密的身份验证版本 2”的选择，选中“可扩展的身份验证协议（EAP），使用智能卡或其他证书”复选框，在弹出的对话框中单击“确定”按钮，然后再次单击“确定”按钮，如图 3-192 所示。

第 3 步，在 ISA Server 管制控制台中，单击“启用 VPN 客户端访问”链接，然后单击“应用”按钮，让设置生效，然后重新启动计算机。

7. 为智能卡用户颁发证书

本节中介绍的智能卡，是一个外形像 U 盘，具有 USB 接口的，可移动的，安全电子设备，如图 3-193 所示。

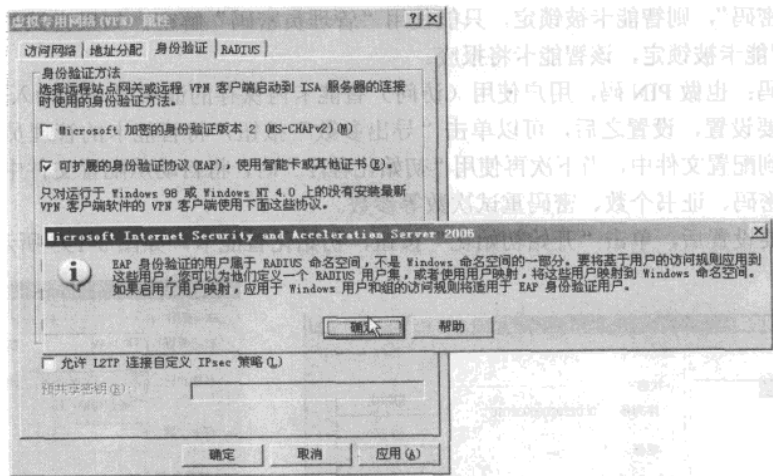


图 3-192 使用智能卡进行验证

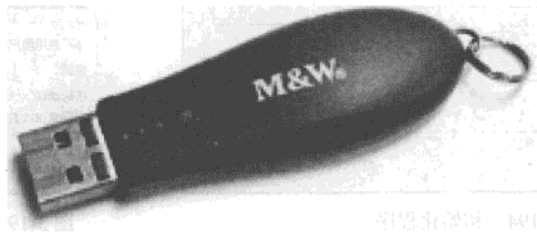


图 3-193 智能卡外形

为智能卡颁发证书的具体步骤如下。

(1) 安装智能卡驱动程序。

在 Windows 2000、Windows XP、Windows Server 2003、Windows Vista 或 Windows Server 2008 中，虽然已经内置了一部分智能卡的驱动程序，但一般情况下用户使用的智能卡，例如本书中介绍的“明华澳汉”智能卡，Windows 操作系统并没有集成该驱动程序，所以，在使用该智能卡前，需要安装智能卡驱动程序。

在企业证书服务器上，安装智能卡驱动程序，在安装驱动程序之前，先不要插入智能卡。有关智能卡驱动程序的安装比较简单，不再过多介绍。

(2) 初始化智能卡。

运行厂家提供的初始化程序，然后插入新的智能卡，如图 3-194 所示。

当智能卡没有初始化时，在“设备清单”中会显示“未初始化 EKEY”提示，单击“初始化”按钮，在弹出的“初始化参数设置”对话框中，设置如下参数：

EKey 卷标：类似于硬盘、软盘的卷标，用来识别或标记智能卡，可以输入 5~16 位字符。

证书个数：设置保存的证书的个数，可以在 1~10 中设置。

管理员密码：设置智能卡的管理员密码，一定要记牢，如果管理员密码丢失，将不能再次初始化智能卡，也不能解密用户密码。

密码重试次数：允许尝试密码的次数，可以在 1~14 中设置。当超过次数时，如果尝试

网管天下 网管经验谈

的是“用户密码”，则智能卡被锁定，只能使用“管理员密码”解密，如果尝试的是“管理员密码”，则智能卡被锁定，该智能卡将报废。

用户密码：也做 PIN 码，用户使用（访问）智能卡内保存的证书时需要输入的密码。

根据需要设置，设置之后，可以单击“导出参数”按钮，将智能卡的管理员密码、用户密码等保存到配置文件中，当下次再使用“初始化程序”时，将自动从配置文件中读取管理员密码、用户密码、证书个数、密码重试次数等参数。

根据需要设置后，单击“开始初始化”按钮，初始化智能卡，如图 3-195 所示。

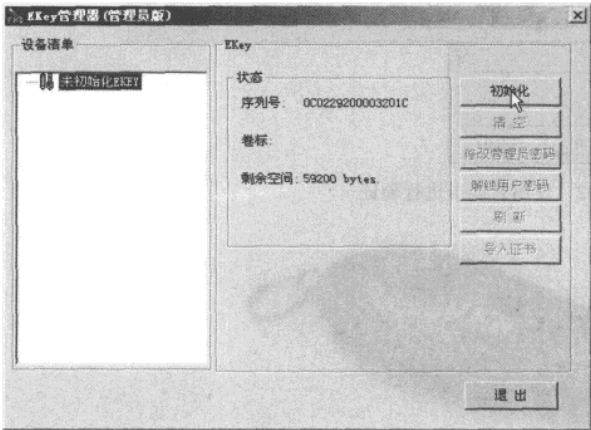


图 3-194 初始化程序

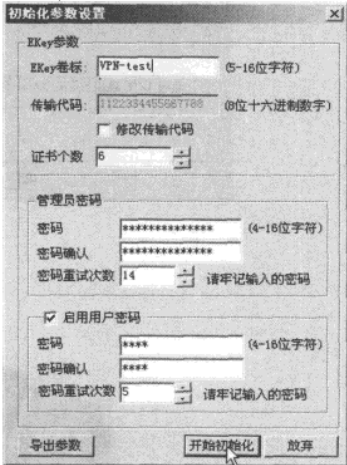


图 3-195 初始化参数设置

初始化成功后，可以拔下当前初始化完成的智能卡，重新插入一个新的智能卡进行初始化的工作。

（3）在企业证书服务器上注册服务。

在默认情况下，企业证书服务器并不能为智能卡颁发证书，需要经过下面的配置才能颁发，步骤如下。

第 1 步，在企业证书服务器上，从“管理工具”中运行“证书颁发机构”，在“证书颁发机构”管理控制台中，右键单击“证书模板”选项，从弹出的快捷菜单中选择“新建”→“要颁发的证书模板”命令，如图 3-196 所示。

第 2 步，在弹出的“启用证书模板”页中，选择“智能卡用户、智能卡登录、注册代理、注册代理（计算机）”选项，然后单击“确定”按钮，如图 3-197 所示。

说
·
明

可以按 Shift、Ctrl 键用鼠标单击进行多选。

第 3 步，关闭“证书颁发机构”窗口，在“运行”中输入 mmc 并按 Enter 键，如图 3-198 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

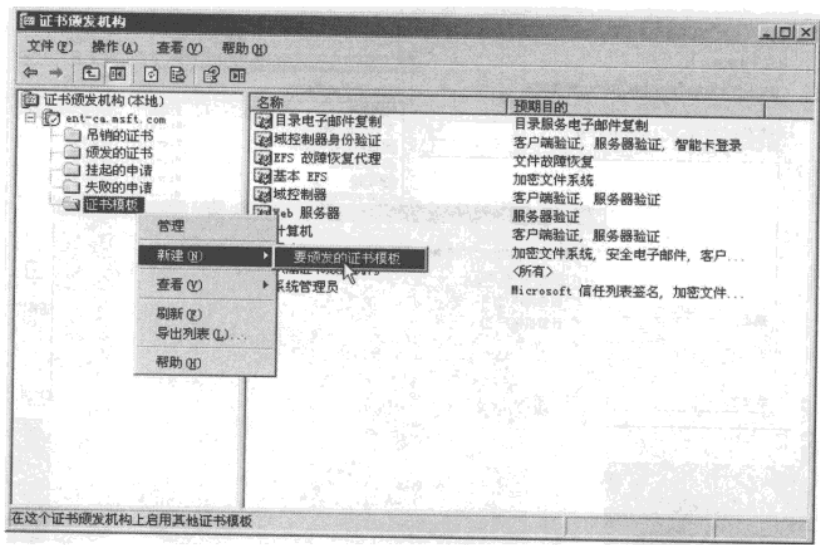


图 3-196 新建证书模板

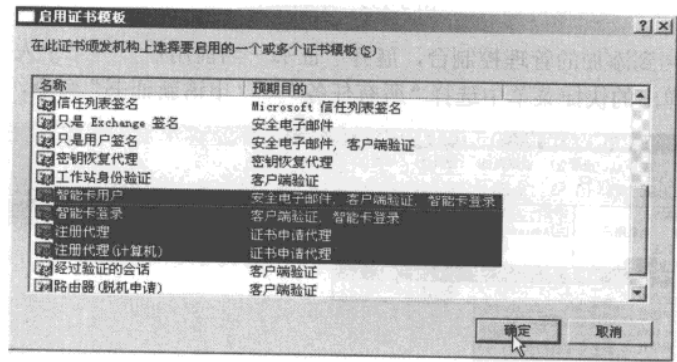


图 3-197 启用证书模板

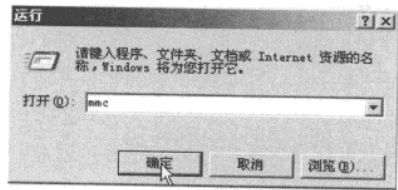


图 3-198 打开控制台

第 4 步，在“控制台 1”窗口中，选择“文件”→“添加/删除管理单元”，在“添加/删除管理单元”对话框中单击“添加”按钮，在弹出的“添加独立管理单元”对话框中双击“证书”选项，在弹出的对话框中选择“我的用户账户”单选按钮，然后单击“完成”按钮，如图 3-199 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

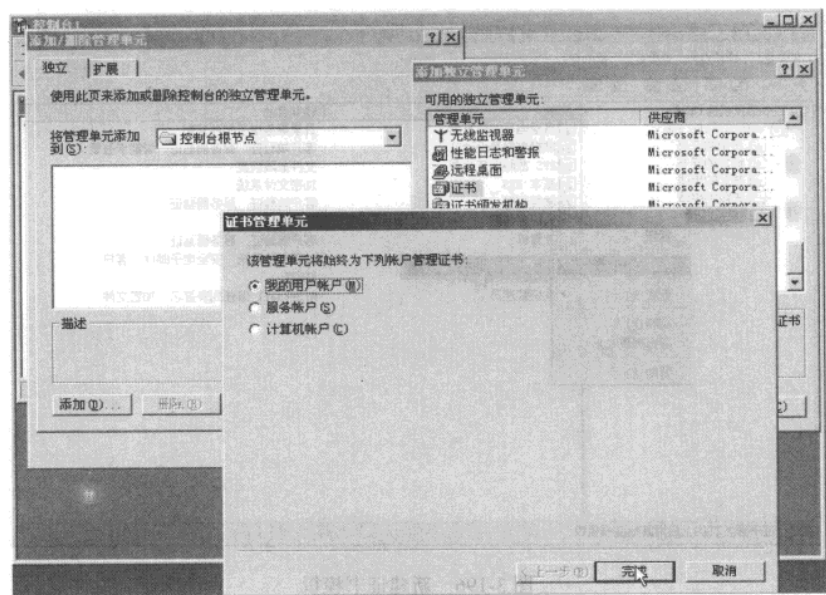


图 3-199 添加证书

第 5 步，返回到添加的管理控制台，展开“证书—当前用户”→“个人”→“证书”，用鼠标右键单击，从弹出的快捷菜单中选择“所有任务”→“申请新证书”命令，如图 3-200 所示。

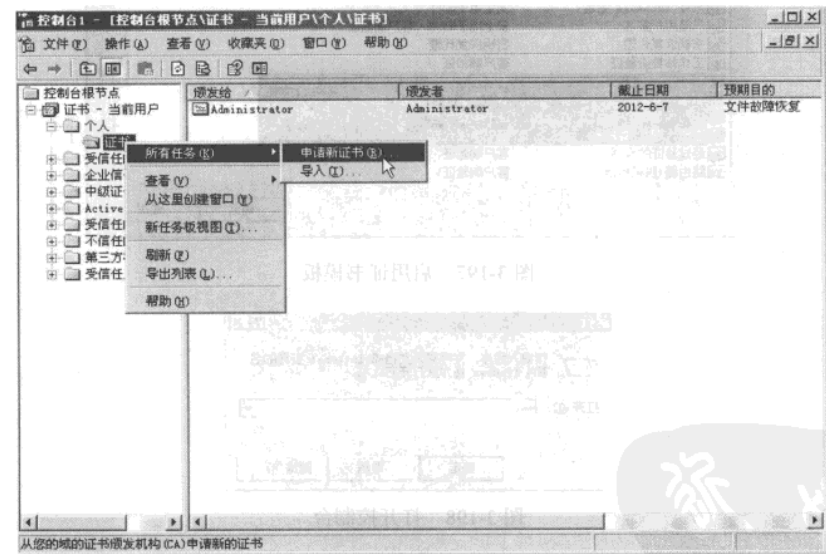


图 3-200 申请证书

第 6 步，在“证书类型”页中，选中“注册代理”选项，如图 3-201 所示。
第 7 步，在“证书的好记的名称和描述”页中，输入名称与描述信息，如图 3-202 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

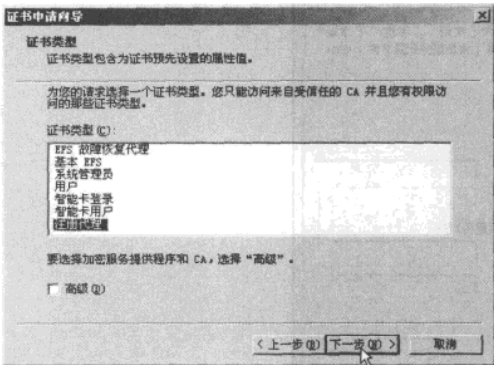


图 3-201 注册代理

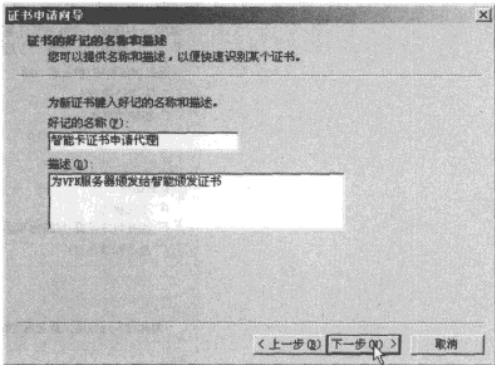


图 3-202 证书名称

第 8 步，在“正在完成证书申请向导”页中，单击“完成”按钮，如图 3-203 所示，完成证书的申请。

(4) 创建用户并为智能卡颁发证书。

在完成上述操作后，就可以为智能卡颁发用户证书了。下面将为用户名为“张三”的用户，颁发智能卡证书，该智能卡将给“张三”使用，步骤如下。

第 1 步，在“Active Directory 用户和计算机”中，创建“张三”用户，并设置“密码永不过期”，如图 3-204 所示。

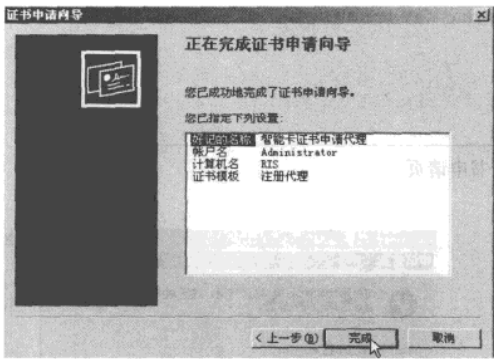


图 3-203 完成证书的申请

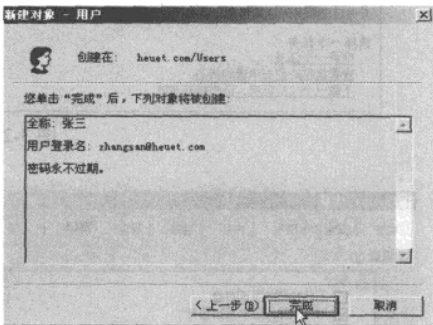


图 3-204 创建账户

第 2 步，在创建账户完成后，设置张三用户属性，允许其有拨入权限，如图 3-205 所示。

第 3 步，打开 IE 浏览器，以管理员账户登录进入证书申请页，为用户申请证书，如图 3-206 所示。在申请之前，需要修改 IE 的设置。

第 4 步，在“高级”选项卡中，选中“允许活动内容在我的计算机上的文件中运行”复选框，如图 3-207 所示。

第 5 步，打开“安全”选项卡，在“受信任的站点”中单击“站点”按钮，将证书服务器的地址添加到列表框中。在添加的时候，取消“对该区域中的所有站点要求服务器验证”复选框，如图 3-208 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

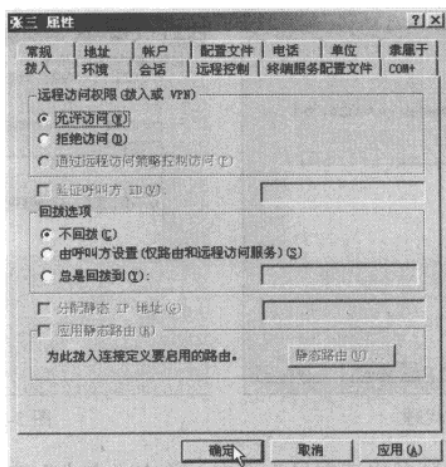


图 3-205 允许访问

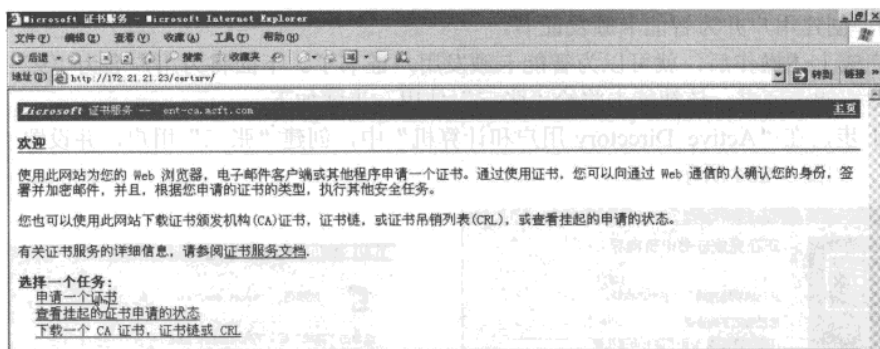


图 3-206 证书申请页

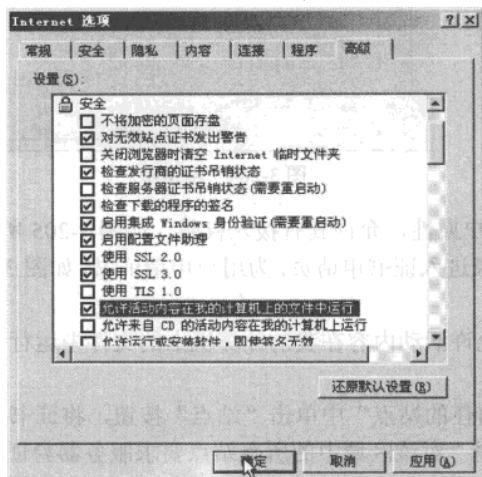


图 3-207 允许活动内容在我的计算机上的文件中运行

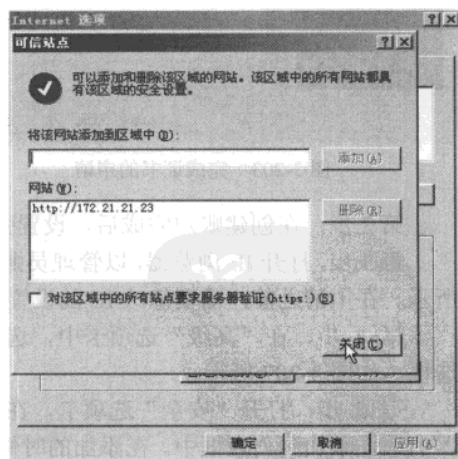


图 3-208 添加受信任站点

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务器方面 | 3

第 6 步，在“高级证书申请”页中，单击“通过使用智能卡证书注册站来为另一用户申请一个智能卡证书”链接，如图 3-209 所示。

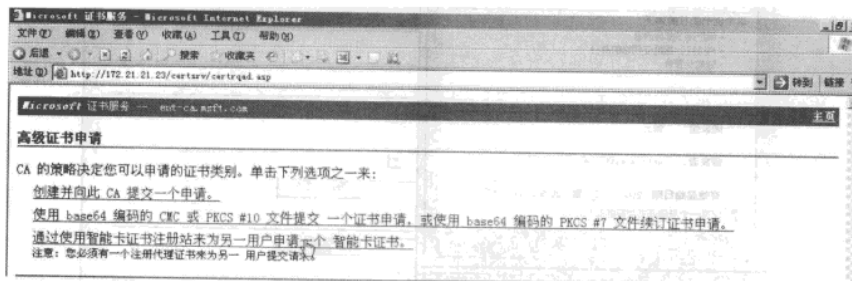


图 3-209 高级证书申请

第 7 步，在弹出的“Internet Explorer”对话框中，单击“是”按钮。

第 8 步，在“证书模板”下拉列表框中选择“智能卡用户”选项，在“加密服务提供程序”下拉列表框中选择“M&W eKey XCSP”选项，然后单击“选择用户”按钮，如图 3-210 所示。

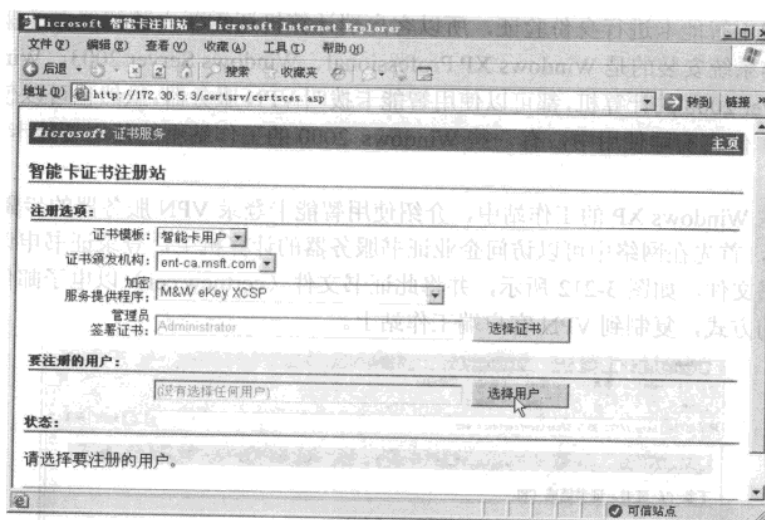


图 3-210 选择用户

第 9 步，在“选择用户”对话框中，输入张三的用户名，然后单击“确定”按钮，返回到图 3-210 后，单击“注册”按钮。

第 10 步，在弹出的“请输入 EKey 访问密码”页中，输入智能卡的用户密码，然后单击“确认”按钮。

第 11 步，注册完成后，单击“查看证书”按钮，查看颁发的证书，如图 3-211 所示。

第 12 步，如果想为其他用户颁发证书，在图 3-211 中单击“新建用户”按钮，插入新的智能卡并为其选择用户，这些操作不再介绍。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

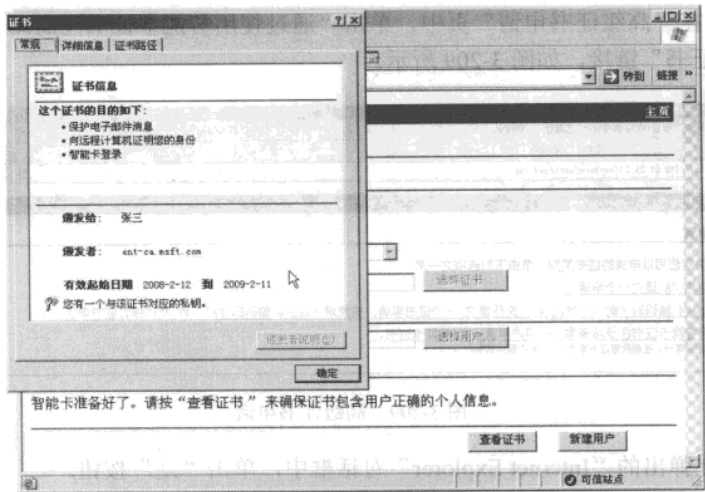


图 3-211 查看颁发的证书

8. 使用智能卡登录到 VPN 服务器

因为要使用智能卡进行身份验证，所以客户端计算机还需要安装智能卡的驱动程序。凡是客户端操作系统安装的是 Windows XP Professional、Windows Server 2003、Windows Vista、Windows Server 2008 的计算机，都可以使用智能卡拨叫 VPN 服务器。虽然也可以使用 Windows 2000 工作站，但在实际使用中，有一些 Windows 2000 的工作站不能使用智能卡访问 VPN 服务器。

下面将在 Windows XP 的工作站中，介绍使用智能卡登录 VPN 服务器的步骤。

第 1 步，首先在网络中可以访问企业证书服务器的计算机上，登录证书申请页，下载并保存 CA 证书文件，如图 3-212 所示，并将此证书文件（certnew.cer）以电子邮件、文件共享或直接复制的方式，复制到 VPN 客户端工作站上。

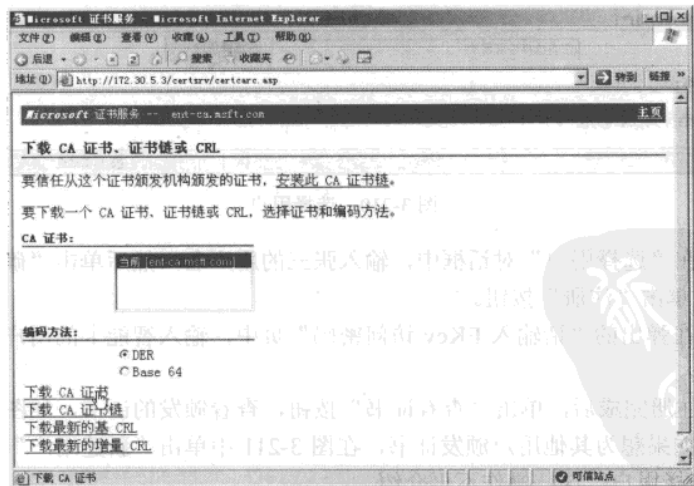


图 3-212 下载 CA 证书

第 2 步，在工作站上双击此证书文件，在弹出的“证书”对话框中，单击“安装证书”按钮，如图 3-213 所示。在“安全警告”对话框中，单击“是”按钮，信任该证书颁发机构。

第 3 步，安装智能卡驱动程序，该步骤十分简单，在此不再赘述。

第 4 步，创建 VPN 拨号连接。在安装智能卡驱动程序后，通过设置 VPN 服务器的 IP 地址会弹出“智能卡”页，在此选择“使用我的智能卡”选项。

第 5 步，创建 VPN 拨号连接完成后，插入智能卡，并使用新创建的 VPN 拨号连接，此时会要求输入智能卡的 PIN，如图 3-214 所示。

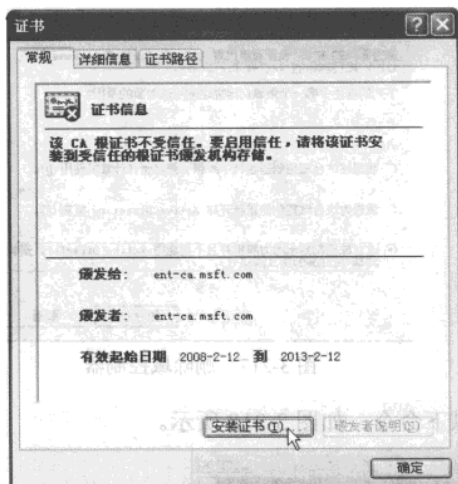


图 3-213 安装证书

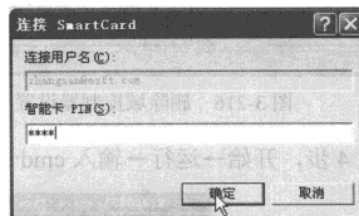


图 3-214 输入智能卡的 PIN

第 6 步，在图 3-214 中输入智能卡的 PIN 码之后，将以智能卡身份验证并拨叫到 VPN 服务器。在第一次拨叫成功时，会弹出“验证服务器证书”对话框，查看之后，单击“确定”按钮，拨叫成功，如图 3-215 所示。

第 7 步，查看 VPN 客户端状态，可以看到“身份验证”是“EAP”。

第 8 步，如果使用以前创建的 VPN 连接，可以进入 VPN 拨号属性，在“安全”选项卡中的“安全选项”中选择“使用智能卡”选项，然后单击“确定”按钮，以后该 VPN 拨号连接时将使用智能卡进行身份验证。

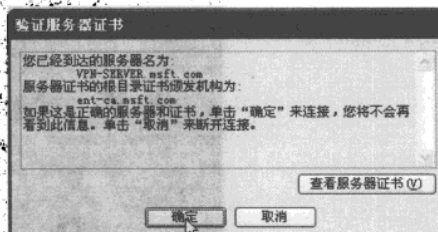


图 3-215 验证服务器证书

3.5.2 手工删除父子域信任关系经验

网络环境说明：父域计算机 ser，子域计算机 app-v，DNS 在 ser 计算机上。

第 1 步，搭建域平台，msft.com 和 w.msft.com 父子域，并产生父子信任关系。

查看：从开始→程序→管理工具→Active Directory 域和信任关系，msft.com 右键→属性→信任，此时信任关系是存在的，但现在删除不了的。下面开始删除父子域关系。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第2步，在 ser 安装 Suptools.msi，该工具可以到 Windows Server 2003 安装光盘找到，路径：\SUPPORT\TOOLS\Suptools.msi。双击安装。

第3步，打开 Active Directory 站点和服务，选中 NTDS Setting，右键单击，在弹出的快捷菜单中选择删除命令，如图 3-216 所示。

选择“这台域控制器永远为肿机并且不再能用 Active Directory 安装向导（DCPROMO）将其降级”单选按钮，如图 3-217 所示。

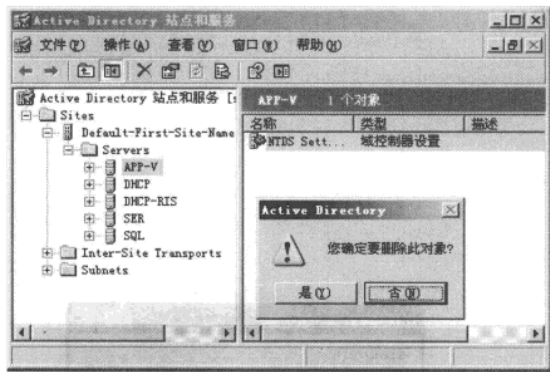


图 3-216 删除域控制器设置

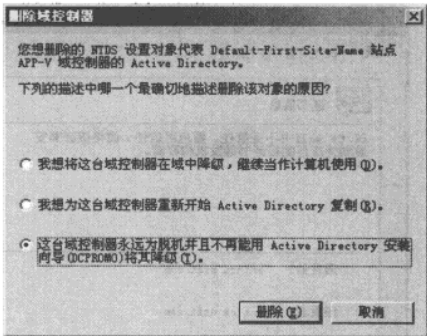


图 3-217 删除域控制器

第4步，开始→运行→输入 cmd→依次输入以下命令，如图 3-218 所示。

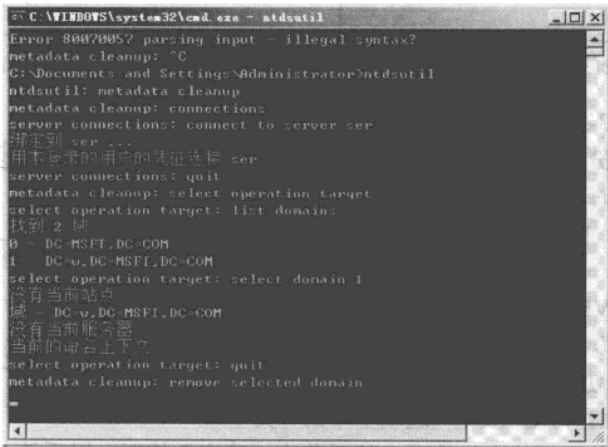


图 3-218 输入命令

第5步，在输入 remove selected domain 命令后会弹出“域删除确认对话框”，单击“是”按钮，如图 3-219 所示。

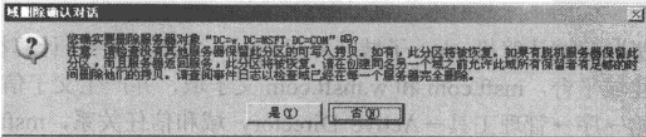


图 3-219 域删除确认

第6步，查看父子域关系是否存在。

从开始→程序→管理工具→Active Directory 域和信任关系，如图 3-220 所示。至此，w.msft.com 已经删除。

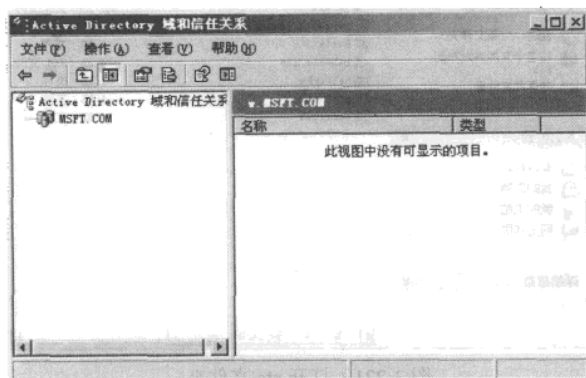


图 3-220 查看域和信任关系

3.5.3 | DNS 服务调教经验

在管理和维护 Windows 服务器的过程中，DNS 服务的设置和维护是其中重要的一项“功课”，毕竟网络访问的高效与否，与 DNS 服务的工作性能息息相关。要让 DNS 服务器始终能为网络访问提供高效服务，自然少不了要掌握一些 DNS 服务的调教技巧。为此，本节特意总结了这方面的一些技巧，希望它们能对各位有所用处。

1. 巧妙查询 DNS 所用端口

有时候需要通过防火墙，来阻止服务器随意接受任意工作站的域名解析请求。不过要实现这个目的，需要事先知道 DNS 使用了什么端口，以及使用了什么通信协议，然后才能在防火墙中针对指定的端口和协议进行过滤设置。那么，如何才能快速地知道 DNS 服务在工作时使用的是什么通信协议及使用的通信端口呢？为此，本文特意为你提供了如下的方法，来快速查询 DNS 所用端口，以及通信协议。

第1步，打开系统的资源管理器窗口，并进入到 Windows 系统所在的安装磁盘分区，再依次展开其中的“Windows”文件夹、“system32”文件夹、“drivers”文件夹、“etc”文件夹，如图 3-221 所示。

接着用鼠标右键单击“etc”文件夹子窗口中的“services”文件，从弹出的快捷菜单中执行“打开方式”命令，在随后出现的“应用程序选择”对话框中，选中“记事本”应用程序，并单击“确定”按钮，如图 3-222 所示。

在其后出现的文本编辑界面中，依次选择工具栏中的“编辑”/“查找”命令，在打开的查找对话框中，输入关键字“Domain Name”，然后单击“查找下一个”按钮，这样你就能在编辑窗口中快速找到域名服务所使用的端口和通信协议了，如图 3-223 所示。从该界面中，不难看出 DNS 所用的通信端口号码为 53，使用的通信协议包括 TCP 协议和 UDP 协议。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

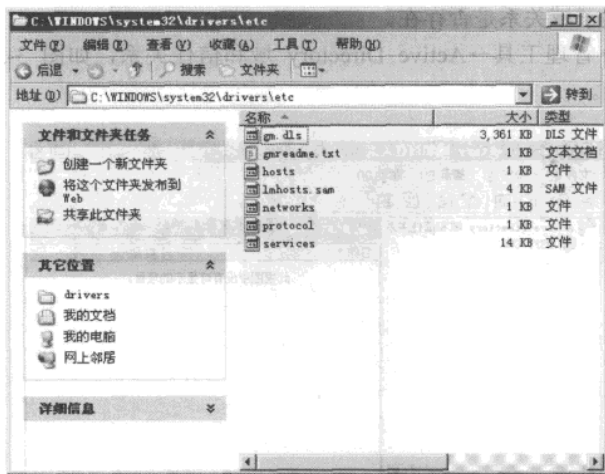


图 3-221 打开 etc 文件夹

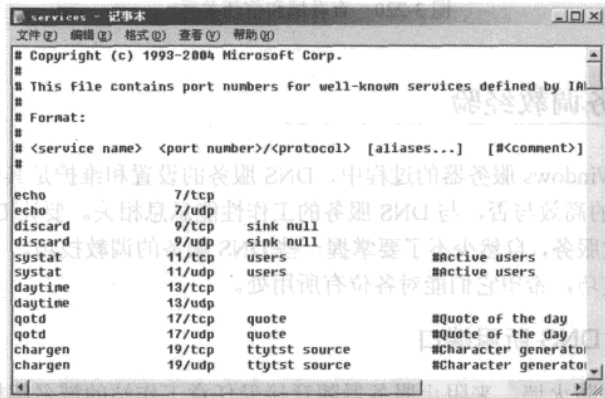


图 3-222 打开 services 文件

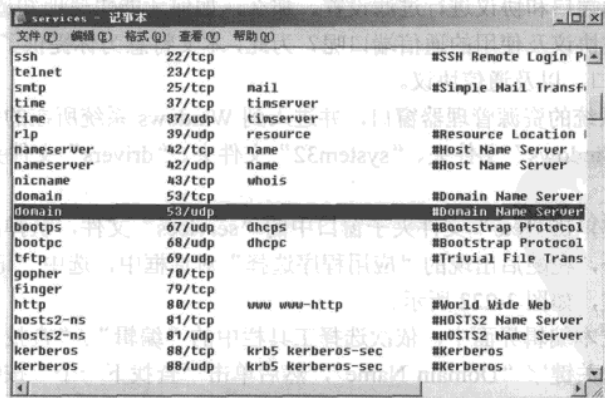


图 3-223 找出域名服务器的协议和端口

2. 快速测试 DNS 的能力

DNS 服务器在进行域名解析时，通常具有简单查询和递归查询两种方式，其中通过简单查询可以知道 DNS 映射一个 IP 地址对应名称的能力大小，通过递归查询可以知道 DNS 映射一个名称对应 IP 地址的能力大小。那么，如何才能快速知道自己搭建的 DNS 服务器，在简单查询能力和递归查询能力方面都有效呢？其实很简单，你只要按照下面的步骤来操作就能知道了。

依次选择“开始”/“程序”/“管理工具”/“DNS”命令，在弹出的 DNS 服务器管理控制台窗口中，用鼠标右键单击目标 DNS 服务器，从随后弹出的右键菜单中执行“属性”命令，如图 3-224 所示。

在接着打开的 DNS 服务器属性设置对话框中，打开“监视”选项卡，并在对应的标签页面中，选中简单查询或递归查询测试选项，再单击“立即测试”按钮，就能对 DNS 服务器的能力进行测试了，如图 3-225 所示。

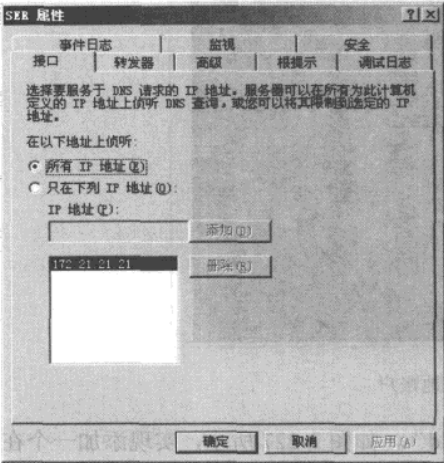


图 3-224 dns 服务器属性

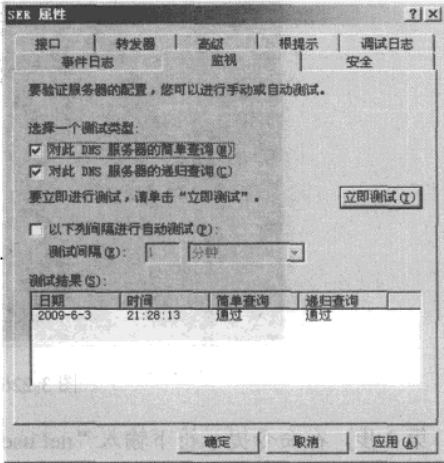


图 3-225 测试 dns 服务器简单查询和递归查询

测试完毕后，你会在对应的窗口中看到具体的结果，例如一旦 DNS 服务器没有递归查询能力的话，测试结果就会表现为“失败”，要是 DNS 服务器具有简单查询功能的话，那么测试结果就会表现为“通过”。当然，如果你选中“以下列间隔进行自动测试”复选框，同时指定好具体的间隔时间的话，那么 Windows 服务器系统就会每隔一定的时间，对 DNS 服务器的简单查询能力或递归查询能力进行自动测试。

3.6 服务器安全管理经验

服务器的安全管理在服务器管理的过程中至关重要。一要防范局域网内的攻击，二要防范 Internet 上的攻击，本节提供了集中常见的方法来防范潜在的安全隐患。其中防止服务器被添加隐藏的账户、限制域用户的并发登录等对防范局域网内的攻击提供了安全保障。而远程登录端口的修改和内置防火墙的设置能够使服务器在 Internet 上免受直接的威胁，保证服务器的

正常运行。

3.6.1 防范服务器被添加隐藏账户的小经验

最近看到了一篇关于“隐藏账户与隐藏权限”方面的文章，觉得对于服务器及客户系统的管理有很大的用处，所以在本节就拿出来也作为一个小经验跟读者分享一下。要想克制敌人，必须先了解敌人，所以要先了解如何添加隐藏账户，以防管理的服务器被人加了特殊权限的隐藏账户，而自己却蒙在鼓里。

接下来就具体介绍一下添加一个隐藏账户与隐藏权限的操作步骤：

第1步，在命令提示符下输入“net user”，如图 3-226 所示，实现查看本地账户的情况的功能。

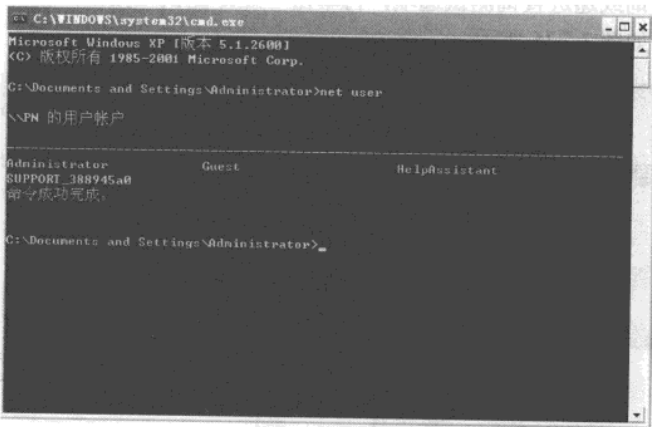


图 3-226 查看本地账户

第2步，在命令提示符下输入“net user pn\$ /add”，如图 3-227 所示，实现添加一个在提示符下看不到的用户 pn\$的功能。

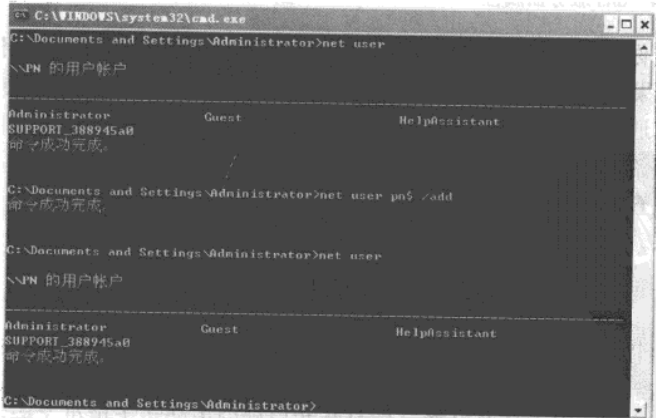


图 3-227 添加隐藏账户 pn\$

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“本地用户和组”中查看，我们可以看到已经添加了测试用的账户“pn\$”，如图 3-228 所示，其组为 Users 组，即为受限账户使用这个账户登录则有很多权限无法操作，例如：修改 Ip 地址等，如图 3-229 所示。

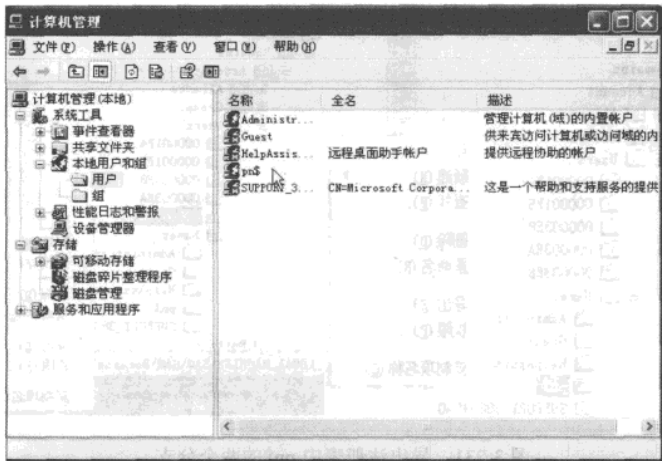


图 3-228 查看本地用户和组

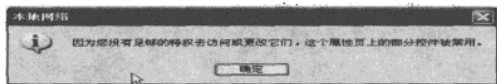


图 3-229 pn\$为受限用户

第 3 步，用 Administrator 用户登录，找到注册表中的分支 SAM（此分支即为系统用户和组在注册表中的位置，对其进行操作，即可修改系统中用户和组的相应权限）。找到 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users 下的 pn\$ 测试用户对应的账户类型中“F”注册表项中的值换成 administrator 账户对应的账户类型中的“F”注册表项中的值，如图 3-230 所示。



图 3-230 修改注册表用户类型值

在“用户和组”中查看用户 pn\$ 仍然为 Users 组的用户，但经测试其权限实为 Administrator 的权限。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 4 步，导出注册表中测试用户 `pn$` 相应的两个分支，如图 3-231 所示，使用命令“`net user pn$ /del`”删除测试用户 `pn$`，如图 3-232 所示。经检查在“本地用户和组”，此用户已经被删除，在注册表中此用户也已被删除。

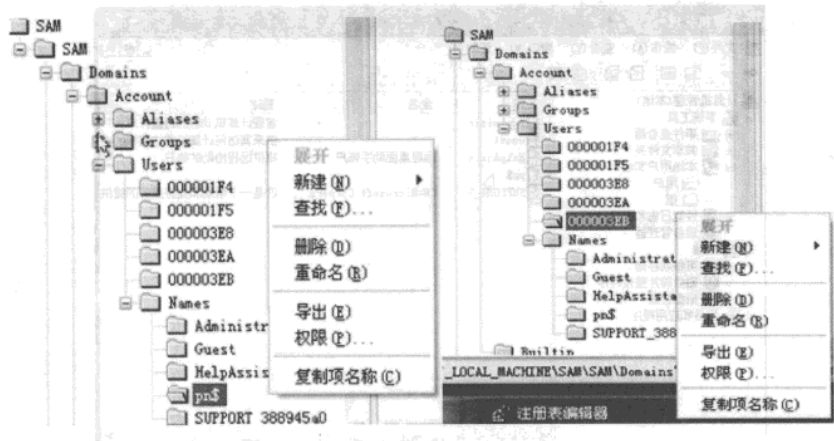


图 3-231 导出注册表中 `pn$` 的两个分支

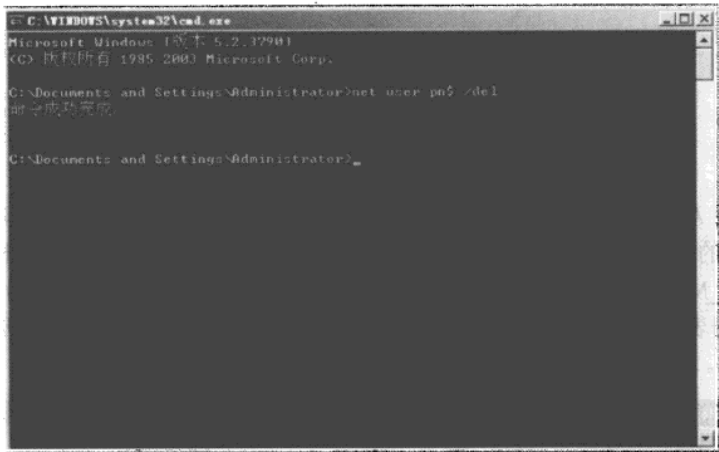


图 3-232 命令提示符下删除 `pn$`

第 5 步，导入刚才导出的测试用户 `pn$` 的注册表文件，可以在注册表中看到刚才删除的测试用户 `pn$`，并且其权限为 Administrator 的权限，如图 3-233 所示。

在“本地用户和组”中却无此用户，如图 3-234 所示，但经过测试可以使用测试用户 `pn$` 登录，并且其权限实为管理员权限。

知道了隐藏账户的创建方法，就不难发现是否有隐藏账户的存在，当然也就可以做到很好的防范准备，防止服务器上有隐藏账户的存在是整个单位网络安全的一个保障。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

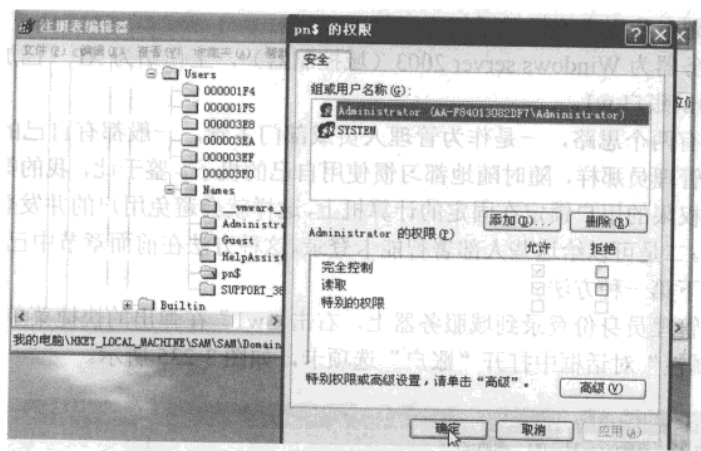


图 3-233 注册表中 pn\$ 账户

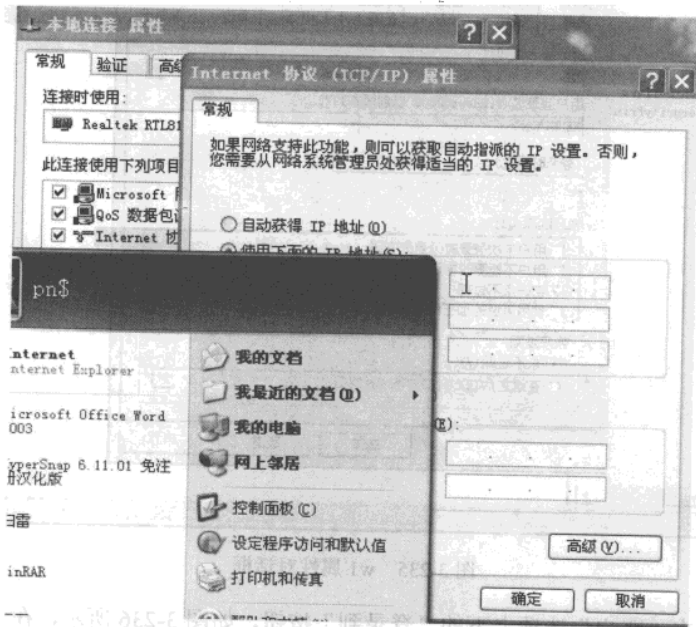


图 3-234 验证隐藏高权限账户创建成功

3.6.2 限制域用户的并发登录的小经验

做网络管理员的人都知道，管理单位网络的杀手锏是给大部分人受限用户，而只有一些部门的主管或是其他有必要的人员设置一些放开权限的账户。我在管理机房时也是这么做的，但是最近发现出了点问题——个别管理员权限的账户被其他人使用了。这件事可大可小，虽然机房没什么机密文件，但想到涉及机密文件的单位的网管就大不相同了，于是我开始摸索着解决这个问题。本节就是跟读者一块分享这方面的一些经验。

网管天下 网管经验谈

为解决该问题，我用虚拟机做了如下实验：

环境为：服务器为 Windows server 2003（域控制器），工作站为 XP（已加入到域中），计算机名 pn，测试账户 w1。

我经过思考有两个思路，一是作为管理人员或部门主管，一般都有自己的计算机而且这些人不会像网络管理员那样，随时随地都习惯使用自己的机子。鉴于此，我的第一个思路就是把这些赋有管理权限的用户锁定在固定的计算机上，这样就会避免用户的并发登录和用户密码泄露造成的困扰。二是可以给这些人部署智能卡登录。这种方法在前面章节中已做了详细介绍。本节就来介绍一下第一种方法。

第 1 步，以管理员身份登录到域服务器上，右击“w1”在弹出的快捷菜单中选择“属性”命令，在“w1 属性”对话框中打开“账户”选项卡，如图 3-235 所示。

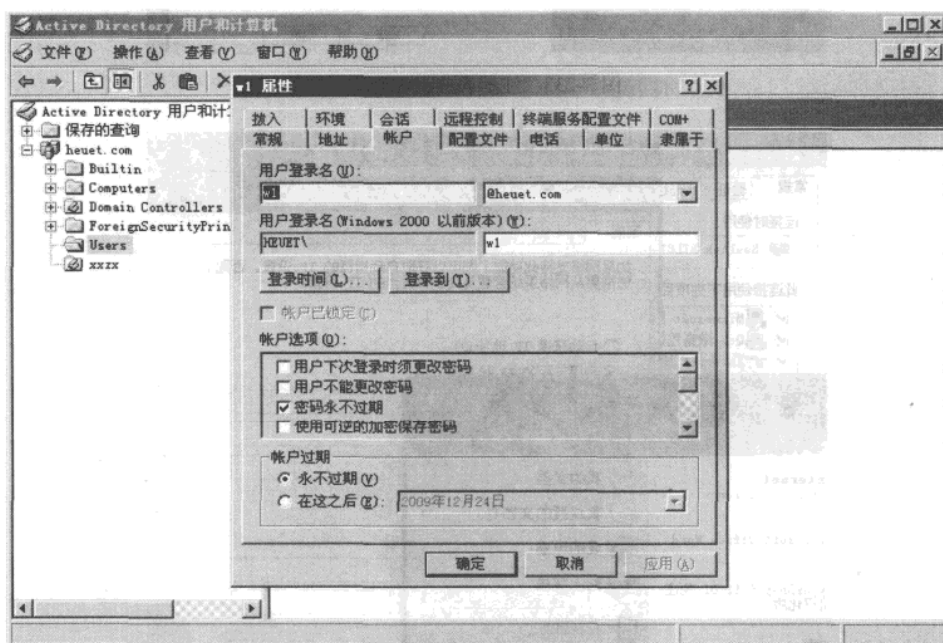


图 3-235 w1 属性对话框

第 2 步，单击“账户”选项卡下的“登录到”按钮，如图 3-236 所示，在“此用户可以登录到”中选中“下列计算机”单选按钮，并在“计算机名”文本框中输入其允许登录的计算机名“pan”，单击“添加”按钮。

第 3 步，经过以上的设定后，w1 这个账户只能够登录到“pan”这台计算机，而不能登录其他计算机。

3.6.3 3389 端口修改

很多管理 Windows 平台下服务器的网管朋友知道，维护服务器都需要远程来执行，有的通过 pcan anywhere，有的用微软提供的 3389 远程连接器。但使用修改端口后的远程终端往往往

服务器方面 | 3

面不流畅，连接速度较慢，甚至百吉吉的带宽也是如此。那到底是什么原因呢？其实是我们修改端口时没修改彻底，才会导致以上情况的发生。以往我们在修改服务器远程终端 3389 端口时，只是修改了 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp 中“PortNumber”的数值，这样也能连接上，但就会造成文章开始说的情况，下面给大家讲解一下具体规范的操作步骤：

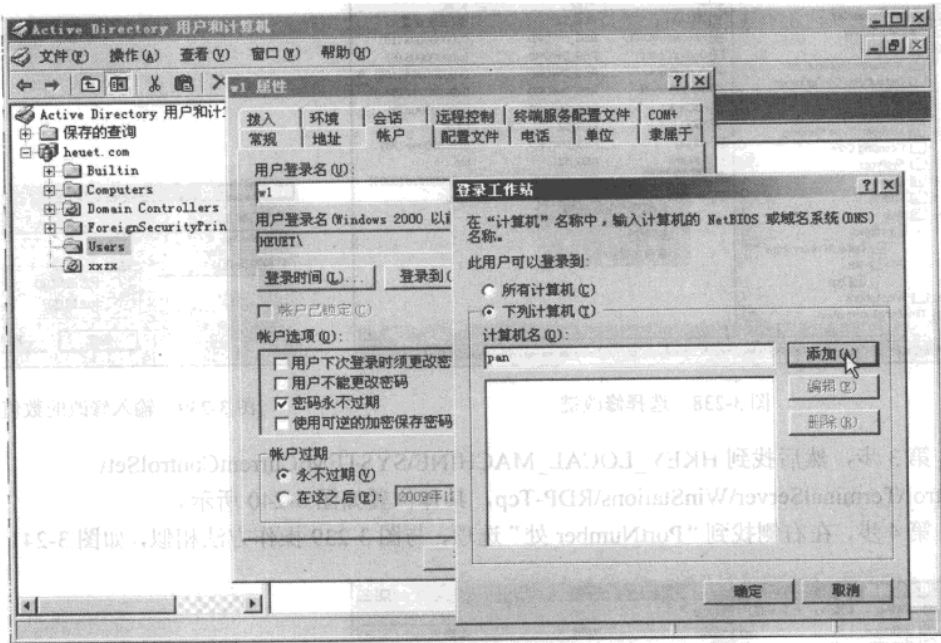


图 3-236 设置域用户登录的计算机

第 1 步，运行里面输入：“regedit”，进入注册表，然后找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 这一项，如图 3-237 所示。

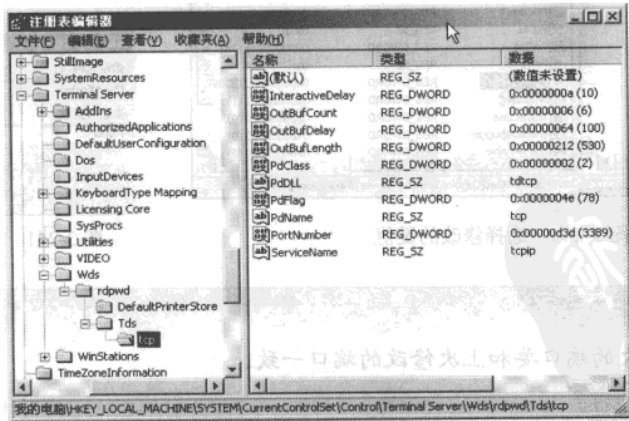


图 3-237 查看注册表项

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

第 2 步，找到“PortNumber”处，鼠标右键选择“修改”，选择十进制，换成你想修改的端口（范围在 1024~65535）而且不能冲突，否则下次就无法正常启动系统了。具体操作方法如图 3-238 和图 3-239 所示。

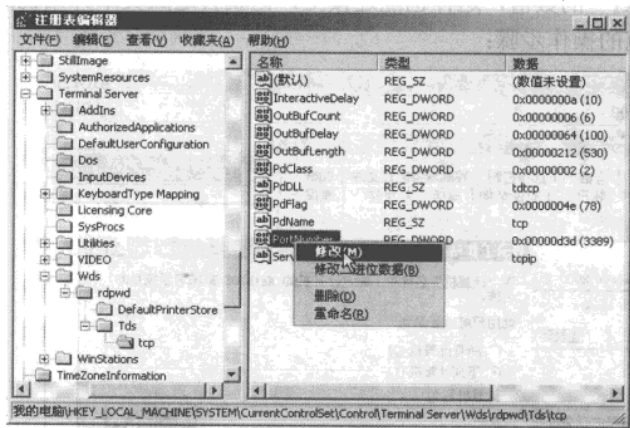


图 3-238 选择修改键

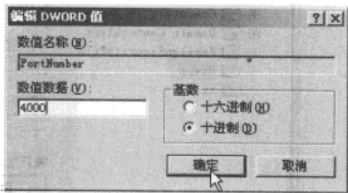


图 3-239 输入修改的数值

第 3 步，然后找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp，具体位置如图 3-240 所示。
第 4 步，在右侧找到“PortNumber”处”选项，与图 3-239 操作方法相似，如图 3-241 所示。

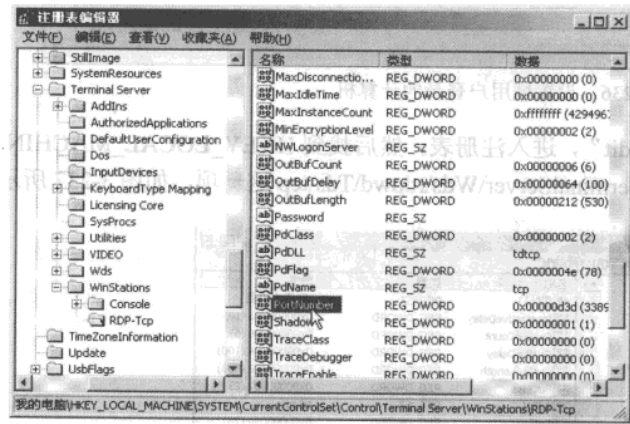


图 3-240 选择修改的键值

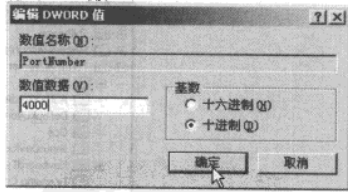


图 3-241 输入要修改的数值

注
意

这次的端口要和上次修改的端口一致。

第 5 步，然后系统重新启动一下，就可以用 3389 连接器远程连接操作了（3389 连接器打

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开方法：Windows XP/2003 中的开始→“运行”窗口中输入“mstsc”即可）。连接的时候格式为 IP:修改后的端口，如图 3-242 所示。

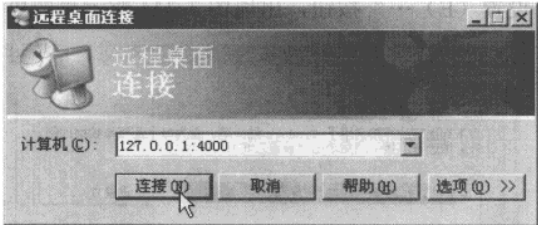


图 3-242 远程桌面连接

3.6.4 Windows 2003 内置的防火墙设置经验

“冲击波”等蠕虫病毒特征之一就是利用有漏洞的操作系统进行端口攻击，因此防范此类病毒的简单方法就是屏蔽不必要的端口，防火墙软件都有此功能，其实对于采用 Windows 2003 或者 Windows XP 的用户来说，不需要安装任何其他软件，因为可以利用系统自带的“Internet 连接防火墙”来防范黑客的攻击。

(1) 基本设置。

第 1 步，鼠标右键单击“网上邻居”选项，在弹出的快捷菜单中选择“属性”命令。

第 2 步，鼠标右键单击“本地连接”选项，在弹出的快捷菜单中选择“属性”命令，出现如图 3-243 所示界面。打开“高级”选项卡，单击“设置”按钮，确定后防火墙即起了作用。

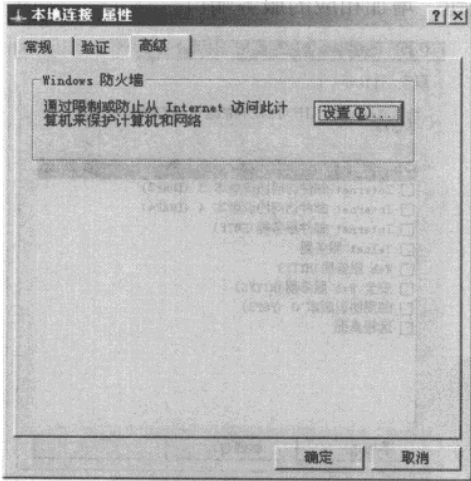


图 3-243 本地连接属性

(2) 测试基本设置。

第 1 步，在另一台计算机上 ping 本机，出现 Request timed out 表示 ping 不通本机。

第 2 步，在另一台计算机上用漏洞扫描工具扫描本机发现没有打开的端口。

网管天下 网管经验谈

这两种测试通过后说明防火墙已经起了作用。

(3) 高级设置。

单击图 3-243 中“设置(E)…”按钮，出现图 3-244 所示界面可进行高级设置。

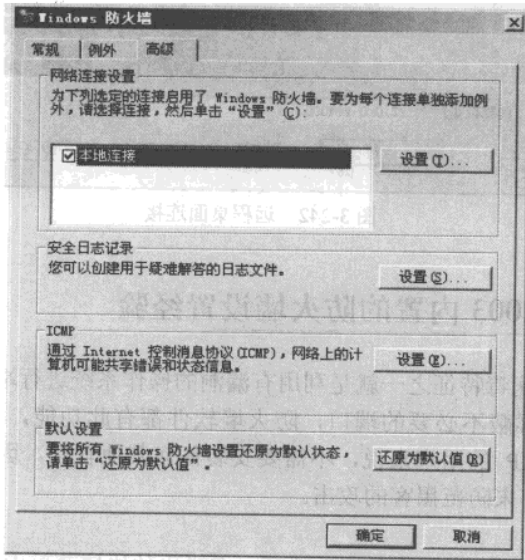


图 3-244 Windows 防火墙

第 1 步，选择要开通的服务，如图 3-245 所示。如果本机要开通相应的服务可选中该服务，本例选中了 FTP 服务，这样从其他计算机就可 FTP 到本机，扫描本机可以发现 21 端口是开放的。可以单击“添加”按钮，增加相应的服务端口。

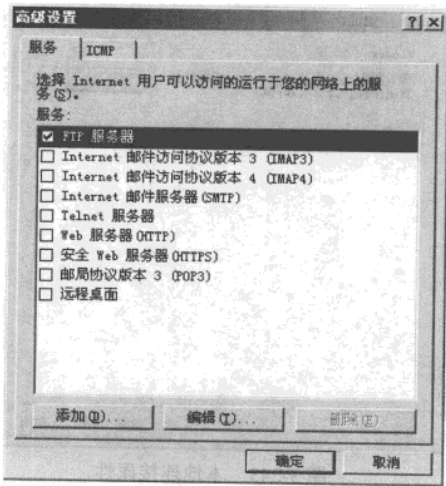


图 3-245 选择开通的服务

第 2 步，设置日志，如图 3-246 所示。选择要记录的项目，防火墙将记录相应的数据，日志默认在 C:/WINDOWS/pfirewall.log，用记事本就可以打开查看。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

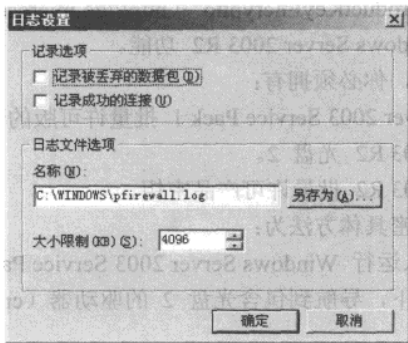


图 3-246 日志设置

第 3 步，设置 ICMP 协议，如图 3-247 所示。最常用的 ping 就是用的 ICMP 协议，默认设置完后 ping 不通本机就是因为屏蔽了 ICMP 协议，如果想 ping 通本机，只需将“允许传入回显请求”一项选中即可。

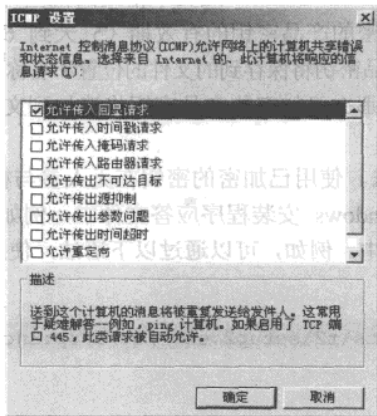


图 3-247 ICMP 设置

3.6.5 | Windows Server 2003 R2 批量许可产品密钥加密

如果你与 Microsoft 签订了批量许可协议（例如 Microsoft Select、Microsoft Enterprise Agreement 和 Microsoft Open License），那么本节内容很适合你。如果要从运行 Windows Server 2003 Service Pack 1 的计算机升级到 Windows Server 2003 R2，那么可以为 Windows Server 2003 R2 批量许可产品密钥加密。此功能通过为产品密钥加密，使其无法以纯文本格式查看，从而增加了一层保护。首先为你的产品密钥加密。然后，可以使用该密钥在无人参与模式下运行 Windows Server 2003 R2 安装程序。

如果要执行 Windows Server 2003 R2 全新安装，那么将需要使用 Windows Server 2003 R2 光盘 1 上提供的加密功能。有关详细信息，请参阅 Microsoft 网站上的“Windows XP

网管天下 网管经验谈

ServicePack1VolumeLicenseProductKeyEncryption” (<http://go.microsoft.com/fwlink?linkId=55330>) (英文)。本文还适用于 Windows Server 2003 R2 功能。

要在升级时使用此功能，你必须拥有：

- 运行 Windows Server 2003 Service Pack 1 批量许可版的计算机。
- Windows Server 2003 R2 光盘 2。
- Windows Server 2003 R2 批量许可产品密钥。

为批量许可产品密钥加密具体方法为：

第 1 步，将光盘 2 插入运行 Windows Server 2003 Service Pack 1 批量许可版的计算机。

第 2 步，在命令提示符下，导航到包含光盘 2 的驱动器（cmpnents\r2\Path\setup2.exe），再运行以下命令：

```
/encryptkey:xxxxx-xxxxx-xxxxx-xxxxx-xxxxx ;  
/encryptdays:NumberOfDays/encryptfile:Filename,
```

实现为产品密钥加密并将其保存到为你 Filename 指定的文件中。

此命令使用的参数：

- xxxxx-xxxxx-xxxxx-xxxxx-xxxxx - 纯文本格式的批量许可产品密钥。
- NumberOfDays-已加密的产品密钥的有效期（5 天到 60 天）。
- Filename-已加密的产品密钥将保存到的文件的位置和名称，例如 C:\Myfolder\Myfile.txt。
如果该文件已存在，那么已加密的产品密钥将追加到文件结尾。应确保你对此位置拥有读写权限。

现在，可以通过下列方法，使用已加密的密钥在无人参与模式下运行安装程序：从命令提示符下；在任何有效的 Windows 安装程序应答文件中，例如 Unattend.txt、Sysprep.inf 或 Ristndrd.sif；或在批处理文件中。例如，可以通过以下语法，使用已加密的密钥在无人参与模式下运行光盘 2。

```
\\Server\share\cmpnents\r2\setup2.exe /q /a /p:EncryptedKey
```

第 4 章 网管员业余管理经验

现在的网络管理不仅要求网管员具有专业的网络知识，还要具有丰富的网络管理经验，掌握一些其他的方法对于网络的管理具有事半功倍的效果。例如在创建大量用户和检查磁盘时要用到 DOS 命令和批处理文件等，这些都能提高管理的效率，还有一些网络管理的软件，往往能使管理员管理起网络来轻松很多。

4.1 网络管理员的基础经验

虽然现在已经是 Windows 时代，但是许多问题处理起来还是需要一些基本的 DOS 命令。本节中将为读者列举了常用的 DOS 命令，希望能够为读者提供方便。另外，本节还介绍了常用的批处理文件的编辑和用法，能够更好的帮助网管员开展网络维护工作。

4.1.1 DOS 命令全集

一、文件管理类命令

（一）MD——建立子目录。

1. 功能：创建新的子目录。
 2. 类型：内部命令。
 3. 格式：MD[盘符:][路径名]〈子目录名〉。
 4. 使用说明：
 - （1）“盘符”：指定要建立子目录的磁盘驱动器字母，若省略，则为当前驱动器。
 - （2）“路径名”：要建立的子目录的上级目录名，若默认则建在当前目录下。
- 例：（1）在 C 盘的根目录下创建名为 FOX 的子目录。
（2）在 FOX 子目录下再创建 USER 子目录。

```
C: \>MD FOX (在当前驱动器 C 盘下创建子目录 FOX)
C: \>MD FOX \USER (在 FOX 子目录下再创建 USER 子目录)
```

（二）CD——改变当前目录。

1. 功能：显示当前目录。
2. 类型：内部命令。
3. 格式：CD[盘符:][路径名][子目录名]。
4. 使用说明：
 - （1）如果省略路径和子目录名则显示当前目录。
 - （2）如采用“CD\”格式，则退回到根目录。
 - （3）如采用“CD..”格式则退回到上一级目录。

网管天下 网管经验谈

- 例：（1）进入到 USER 子目录。
（2）从 USER 子目录退回到子目录。
（3）返回到根目录。

```
C:\>CD FOX \USER (进入 FOX 子目录下的 USER 子目录)
C:\FOX\USER>CD (退回上一级根目录)
C:\FOX>CD\ (返回到根目录)
C:\>
```

（三）RD——删除子目录命令。

1. 功能：从指定的磁盘删除子目录。
2. 类型：内部命令。
3. 格式：RD[盘符：][路径名][子目录名]。
4. 使用说明：

（1）子目录在删除前必须是空的，也就是说需要先进入该子目录，使用 DEL（删除文件的命令）将其子目录下的文件删空，然后再退回到上一级目录，用 RD 命令删除该子目录本身。

（2）不能删除根目录和当前目录。

例：要求把 C 盘 FOX 子目录下的 USER 子目录删除，操作如下：

第 1 步：先将 USER 子目录下的文件删空。

```
C:\>DEL C:\FOX\USER\*.*
```

第 2 步，删除 USER 子目录。

```
C:\>RD C:\FOX\USER
```

（四）DIR——显示磁盘目录命令。

1. 功能：显示磁盘目录的内容。
2. 类型：内部命令。
3. 格式：DIR [盘符][路径][P][W]。

使用说明：/P 的使用：当欲查看的目录太多，无法在一屏显示完屏幕会一直往上卷，不容易看清，加上/P 参数后，屏幕上会分面一次显示 23 行的文件信息，然后暂停，并提示：“Press any key to continue”。

/W 的使用：加上/W 只显示文件名，至于文件大小及建立的日期和时间则都省略。加上参数后，每行可以显示五个文件名。

（五）PATH——路径设置命令。

1. 功能：设备可执行文件的搜索路径，只对文件有效。
2. 类型：内部命令。
3. 格式：PATH[盘符 1]目录[路径名 1][{；盘符 2：}，〈目录路径名 2〉…}。
4. 使用说明：

（1）当运行一个可执行文件时，DOS 会先在当前目录中搜索该文件，若找到则运行之；若找不到该文件，则根据 PATH 命令所设置的路径，顺序逐条地到目录中搜索该文件。

（2）PATH 命令中的路径，若有两条以上，各路径之间以一个分号“；”隔开。

(3) PATH 命令有三种使用方法：

PATH[盘符 1:][路径 1][盘符 2:][路径 2]...（设定可执行文件的搜索路径）。

PATH:（取消所有路径）。

PATH:（显示目前所设的路径）。

(六) TREE——显示磁盘目录结构命令。

1. 功能：显示指定驱动器上所有目录路径和这些目录下的所有文件名。

2. 类型：外部命令。

3. 格式：TREE[盘符:][[/F]] [PRN]。

4. 使用说明：

(1) 使用/F 参数时显示所有目录及目录下的所有文件，省略时，只显示目录，不显示目录下的文件。

(2) 选用>PRN 参数时，则把所列目录及目录中的文件名打印输出。

(七) DELTREE——删除整个目录命令。

1. 功能：将整个目录及其下子目录和文件删除。

2. 类型：外部命令。

3. 格式：DELTREE[盘符:] (路径名)。

4. 使用说明：该命令可以一步就将目录及其下的所有文件、子目录、更下层的子目录一并删除，而且不管文件的属性为隐藏、系统或只读，只要该文件位于删除的目录之下，DELTREE 都一视同仁，照删不误，使用时务必小心。

二、磁盘操作类命令

(一) FORMAT——磁盘格式化命令。

1. 功能：对磁盘进行格式化，划分磁道和扇区；同时检查出整个磁盘上有无带缺陷的磁道，对坏道加注标记；建立目录区和文件分配表，使磁盘做好接收 DOS 的准备。

2. 类型：外部命令。

3. 格式：FORMAT (盘符:) [/S]/[4]/[Q]。

4. 使用说明：

(1) 命令后的盘符不可默认，若对硬盘进行格式化，则会如下列提示：

```
WARNING:ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)?
```

（警告：所有数据在 C 盘上，将会丢失，确实要继续格式化吗？）

(2) 若是对软盘进行格式化，则会如下提示：

```
Insert new diskette for drive A;
and press ENTER when ready...
```

（在 A 驱中插入新盘，准备好后按 Enter 键）。

(3) 选用/S 参数，将把 DOS 系统文件 IO.SYS、MSDOS.SYS 及 COMMAND.COM 复制到磁盘上，使该磁盘可以作为 DOS 启动盘。若不选用/S 参数，则格式化后的磁盘只能读写信息，而不能做为启动盘。

网管天下 网管经验谈

(4) 选用[/4]参数，在 1.2 MB 的高密度软驱中格式化 360KB 的低密度盘。

(5) 选用[/Q]参数，快速格式化，这个参数并不会重新划分磁盘的磁道和扇区，只能将磁盘根目录、文件分配表和引导扇区清成空白，因此，格式化的速度较快。

(6) 选用[/U]参数，表示无条件格式化，即破坏原来磁盘上所有数据。不加/U，则为安全格式化，这时先建立一个镜像文件保存原来的 FAT 表和根目录，必要时可用 UNFORMAT 恢复原来的数据。

(二) UNFORMAT 恢复格式化命令。

1. 功能：对进行过格式化误操作丢失数据的磁盘进行恢复。

2. 类型：外部命令。

3. 格式：UNFORMAT [盘符] [/L] [/U] [/P] [/TEST]。

4. 使用说明：用于将被“非破坏性”格式化的磁盘恢复。根目录下被删除的文件或子目录及磁盘的系统扇区（包括 FAT、根目录、BOOT 扇区及硬盘分区表）受损时，也可以用 UNFORMAT 来抢救。

(1) 选用/L 参数列出找到的子目录名称、文件名称、大小日期等信息，但不会真的做 FORMAT 工作。

(2) 选用/P 参数将显示于屏幕的报告（包含/L 参数所产生的信息）同时也送到打印机。运行时屏幕会显示：

```
Print out will be sent to LPT1
```

(3) 选用/TEST 参数只做模拟试验（TEST）不做真正的写入动作。使用此参数屏幕会显示：“Simulation only”

(4) 选用/U 参数不使用 MIRROR 映像文件的数据，直接根据磁盘现状进行 UNFORMAT。

(5) 选用/PSRTN；修复硬盘分区表。

若在盘符之后加上/P、/L、/TEST 之一，都相当于使用了/U 参数，UNFORMAT 会“假设”此时磁盘没有 MIRROR 映像文件。

注意

UNFORMAT 对于 FORMAT 的磁盘，可以完全恢复，但 FORMAT 后若做了其他数据的写入，则 UNFORMAT 就不能完整的救回数据了。UNFORMAT 并非万能的，由于使用 UNFORMAT 会重建 FAT 与根目录，所以它也具有较高的危险性，操作不当可能会扩大损失，如果仅误删了几个文件或子目录，只需要利用 UNDELETE 就够了。

(三) CHKDSK——检查磁盘当前状态命令。

1. 功能：显示磁盘状态、内存状态和指定路径下指定文件的不连续数目。

2. 类型：外部命令。

3. 格式：CHKDSK [盘符] [路径][文件名] [/F] [/V]。

4. 使用说明：

(1) 选用[文件名]参数，则显示该文件占用磁盘的情况。

(2) 选[/F]参数，纠正在指定磁盘上发现的逻辑错误。

(3) 选用[/V]参数，显示盘上的所有文件和路径。

（四）DISKCOPY——整盘复制命令。

1. 功能：复制格式和内容完全相同的软盘。
2. 类型：外部命令。
3. 格式：DISKCOPY[盘符 1:][盘符 2:]。
4. 使用说明：
 - （1）如果目标软盘没有格式化，则复制时系统自动进行格式化。
 - （2）如果目标软盘上原有文件，则复制后将全部丢失。
 - （3）如果是单驱动器复制，系统会提示适时更换源盘和目标盘，请操作时注意分清源盘和目标盘。

（五）LABEL——建立磁盘卷标命令。

1. 功能：建立、更改、删除磁盘卷标。
2. 类型：外部命令。
3. 格式：LABEL[盘符:][卷标名]。
4. 使用说明：
 - （1）卷标名为要建立的卷标名，若默认此参数，则系统提示输入卷标名或询问是否删除原有的卷标名。
 - （2）卷标名由 1 至 11 个字符组成。

（六）VOL——显示磁盘卷标命令

1. 功能：查看磁盘卷标号。
2. 类型：内部命令。
3. 格式：VOL[盘符:]。
4. 使用说明：省略盘符，显示当前驱动器卷标。

（七）SCANDISK——检测、修复磁盘命令

1. 功能：检测磁盘的 FAT 表、目录结构、文件系统等是否有问题，并可检测出的问题加以修复。
2. 类型：外部命令。
3. 格式：SCANDISK[盘符 1:][[盘符 2:]...][ALL]。
4. 使用说明：
 - （1）CCANDISK 适用于硬盘和软盘，可以一次指定多个磁盘或选用[ALL]参数指定所有的磁盘。
 - （2）可自动检测出磁盘中所发生的交叉连接、丢失簇和目录结构等逻辑上的错误，并加以修复。

（八）DEFRAG——重整磁盘命令。

1. 功能：整理磁盘，消除磁盘碎片。
2. 类型：外部命令。
3. 格式：DEFRAG[盘符:][/F]。
4. 使用说明：选用/F 参数，将文件中存在盘上的碎片消除，并调整磁盘文件的安排，确保文件之间毫无空隙。从而加快读盘速度和节省磁盘空间。

（九）SYS——系统复制命令。

1. 功能：将当前驱动器上的 DOS 系统文件 IO.SYS, MSDOS.SYS 和 COMMAND.COM 传

网管天下 网管经验谈

送到指定的驱动器上。

2. 类型：外部命令。

3. 格式：SYS[盘符：]。

使用说明：如果磁盘剩余空间不足以存放系统文件，则提示：

No room for on destination disk

三、文件操作类命令

（一）COPY 文件复制命令。

1. 功能：复制一个或多个文件到指定盘上。

2. 类型：内部命令。

3. 格式：COPY [源盘][路径]〈源文件名〉[目标盘][路径][目标文件名]。

4. 使用说明：

（1）COPY 是文件对文件的方式复制数据，复制前目标盘必须已经格式化。

（2）复制过程中，目标盘上相同文件名称的旧文件会被源文件取代。

（3）复制文件时，必须先确定目标盘有足够的空间，否则会出现 insufficient 的错误信息，提示磁盘空间不够。

（4）文件名中允许使用通配符“*”“？”，可同时复制多个文件。

（5）COPY 命令中源文件名必须指出，不可以省略。

（6）复制时，目标文件名可以与源文件名相同，称做“同名复制”，此时目标文件名可以省略。

（7）复制时，目标文件名也可以与源文件名不相同，称做“异名复制”，此时，目标文件名不能省略。

（8）复制时，还可以将几个文件合并为一个文件，称为“合并复制”，格式如下：COPY；[源盘][路径]〈源文件名 1〉〈源文件名 2〉…[目标盘][路径]〈目标文件名〉。

（9）利用 COPY 命令，还可以从键盘上输入数据建立文件，格式如下：COPY CON [盘符：][路径]〈文件名〉。

（10）注意：COPY 命令的使用格式，源文件名与目标文件名之间必须有空格。

（二）XCOPY——目录复制命令。

1. 功能：复制指定的目录和目录下的所有文件连同目录结构。

2. 类型：外部命令。

3. 格式：XCOPY [源盘：]〈源路径名〉[目标盘符：][目标路径名][/S][/V][/E]。

4. 使用说明。

（1）XCOPY 是 COPY 的扩展，可以把指定的目录连文件和目录结构一并复制，但不能复制隐藏文件和系统文件。

（2）使用时源盘符、源目标路径名、源文件名至少指定一个。

（3）选用/S 时对源目录下及其子目录下的所有文件进行 COPY。除非指定/E 参数，否则/S 不会复制空目录，若不指定/S 参数，则 XCOPY 只复制源目录本身的文件，而不涉及其下的子目录。

（4）选用/V 参数时，对复制的扇区都进行校验，但速度会降低。

（三）TYPE——显示文件内容命令

1. 功能：显示 ASCII 码文件的内容。
2. 类型：内部命令。
3. 格式：TYPE[盘符：][路径]〈文件名〉。
4. 使用说明：

（1）显示由 ASCII 码组成的文本文件，对 EXE.COM 等为扩展名的文件，其显示的内容是无法阅读的，没有实际意义。

（2）该命令一次只可以显示一个文件的内容，不能使用通配符。

（3）如果文件有扩展名，则必须将扩展名写上。

（4）当文件较长，一屏显示不下时，可以按以下格式显示：TYPE[盘符：][路径]〈文件名〉|MORE，MORE 为分屏显示命令，使用这些参数后当满屏时会暂停，按任意键会继续显示。

（5）若需将文件内容打印出来，可用如下格式：

TYPE[盘符：][路径]〈文件名〉，>PRN

此时，打印机应处于联机状态。

（四）REN——文件改名命令。

1. 功能：更改文件名称。
2. 类型：内部命令。
3. 格式：REN[盘符：][路径]〈旧文件名〉〈新文件名〉。
4. 使用说明：

（1）新文件名前不可以加上盘符和路径，因为该命令只能对同一盘上的文件更换文件名。

（2）允许使用通配符更改一组文件名或扩展名。

（五）FC——文件比较命令。

1. 功能：比较文件的异同，并列出差异处。
2. 类型：外部命令。
3. 格式：FC[盘符：][路径名]〈文件名〉[盘符：][路径名][文件名][/A][/B][/C][/N]。
4. 使用说明：

（1）选用/A 参数，为 ASCII 码比较模式。

（2）选用/B 参数，为二进制比较模式。

（3）选用/C 参数，将大小写字符看成是相同的字符。

（4）选用/N 参数，在 ASCII 码比较方式下，显示相异处的行号。

（六）ATTRIB——修改文件属性命令。

1. 功能：修改指定文件的属性。
2. 类型：外部命令。
3. 格式：ATTRIB[文件名][R][—R][A][—A][H][—H][S][—S][S]。
4. 使用说明：

（1）选用 R 参数，将指定文件设为只读属性，使得该文件只能读取，无法写入数据或删除；选用 —R 参数，去除只读属性。

（2）选用 A 参数，将文件设置为档案属性；选用 —A 参数，去除档案属性。

（3）选用 H 参数，将文件调协为隐含属性；选用 —H 参数，去除隐含属性。

网管天下 网管经验谈

(4) 选用 S 参数，将文件设置为系统属性；选用——S 参数，去除系统属性。

(5) 选用/S 参数，对当前目录下的所有子目录进行设置。

(七) DEL——删除文件命令。

1. 功能：删除指定的文件。

2. 类型：内部命令。

3. 格式：DEL[盘符：][路径]〈文件名〉[P]。

4. 使用说明：

(1) 选用/P 参数，系统在删除前询问是否真要删除该文件，若不使用这个参数，则自动删除。

(2) 该命令不能删除属性为隐含或只读的文件。

(3) 在文件名称中可以使用通配符。

(4) 若要删除磁盘上的所有文件（DEL*.*或 DEL.），则会提示：（Are you sure？）（你确定吗？）若回答 Y，则进行删除，回答 N，则取消此次删除作业。

(八) UNDELETE——恢复删除命令。

1. 功能：恢复被误删除命令。

2. 类型：外部命令。

3. 格式：UNDELETE[盘符：][路径名]〈文件名〉[/DOS]/LIST[/ALL]。

4. 使用说明：使用 UNDELETE 可以使用“*”和“？”通配符。

(1) 选用/DOS 参数 根据目录里残留的记录来恢复文件。由于文件被删除时，目录所记载文件名第一个字符会被改为 E5，DOS 即依据文件开头的 E5 和其后续的字符来找到欲恢复的文件，所以，UNDELETE 会要求用户输入一个字符，以便将文件名字补齐。但此字符不必和原来的一样，只需符合 DOS 的文件名规则即可。

(2) 选用/LIST 只“列出”符合指定条件的文件而不做恢复，所以对磁盘内容完全不会有影响。

(3) 选用/ALL 自动将可完全恢复的文件完全恢复，而不一一地询问用户，使用此参数时，若 UNDELTE 利用目录里残留的记录来将文件恢复，则会自动选一个字符将文件名补齐，并且使其不与现存文件名相同，选用字符的优选顺序为：#%——0000123456789A~Z。

四、其他命令

(一) CLS——清屏幕命令。

1 功能：清除屏幕上的所有显示，光标置于屏幕左上角。

2 类型：内部命令。

3 格式：CLS。

(二) VER 查看系统版本号命令。

1 功能：显示当前系统版本号。

2 类型：内部命令。

3 格式：VER。

(三) DATA 日期设置命令。

1 功能：设置或显示系统日期。

2 类型：内部命令。

3 格式：DATE[mm—dd—yy]。

4 使用说明：

(1) 省略[mm—dd—yy]显示系统日期并提示输入新的日期，不修改则可直接按 Enter 键，[mm—dd—yy]为“月月—日日—年年”格式。

(2) 当计算机开始启动时，有自动批处理文件（AUTOEXEC.BAT）被执行，则系统不提示输入系统日期。否则，提示输入新日期和时间。

(四) TIME 系统时钟设置命令。

1 功能：设置或显示系统时期。

2 类型：内部命令。

3 格式：TIME[hh: mm: ss: xx]。

4 使用说明：

(1) 省略[hh: mm: ss: xx]，显示系统时间并提示输入新的时间，不修改则可直接按 Enter 键，[hh: mm: ss: xx]为“小时：分钟：秒：百分之几秒”格式。

(2) 当计算机开始启动时，有自动批处理文件（AUTOEXEC.BAT）被执行，则系统不提示输入系统日期。否则，提示输入新日期和时间。

(五) MEM 查看当前内存状况命令。

1 功能：显示当前内存使用的情况。

2 类型：外部命令。

3 格式：MEM[/C]/[F]/[M]/[P]。

4 使用说明。

(1) 选用/C 参数列出装入常规内存和 CMB 的各文件的长度，同时也显示内存空间的使用状况和最大的可用空间。

(2) 选用/F 参数分别列出当前常规内存剩余的字节大小和 UMB 可用的区域及大小。

(3) 选用/M 参数显示该模块使用内存地址、大小及模块性质。

(4) 选用/P 参数指定当输出超过一屏时，暂停供用户查看。

(六) MSD 显示系统信息命令。

1 功能：显示系统的硬件和操作系统的状况。

2 类型：外部命令。

3 格式：MSD[/I]/[B]/[S]。

4 使用说明：

(1) 选用/I 参数时，不检测硬件。

(2) 选用/B 参数时，以黑白方式启动 MSD。

(3) 选用/S 参数时，显示出简明的系统报告。

4.1.2 | DOS 批处理文件

DOS 下的可执行文件有 3 种，分别是 EXE、COM 和 BAT。其中，EXE 和 COM 文件都是二进制形式的，只有 BAT 文件是文本形式的，可以直接阅读。因此，BAT 文件和以上二进制可执行文件相比，内容要简单的多。这些文件内包含着 DOS 命令的集合，通常叫做批处理文件。批处理文件的组成虽然比较简单，但其用处非常大，使用也比较广泛。比如每次都执行

网管天下 网管经验谈

一些相同的命令，你一定会觉得非常麻烦，而放在批处理文件中执行时则轻松得多。AUTOEXEC.BAT 就是一个特殊的批处理文件，它在 DOS 的启动时自动运行，在系统的配置中发挥着非常大的作用。因此，要学好 DOS，就要学好批处理文件。下面介绍批处理文件的命令及其使用。

@：将这个符号放在批文件中其他命令的前面，运行时将不显示命令本身。

如@ECHO OFF 命令就在批文件首经常用到。

CALL：从一个批文件中调用另一个批文件，调用完后继续执行原来的批文件。

用法：CALL [批文件名]。

注：也可以使用 COMMAND /C 命令完成同样的操作。

CHOICE：选择命令。这是一个 DOS 外部命令，但它主要用在批文件中。

CHOICE 命令执行后将提示可选择的项目，这时通过一个按键来选择。

用法：CHOICE：[/C[:按键表]] [/N] [/S] [/T[:选择值,秒数]] [显示文本]

其中，/C 表示可选择的按键，/N 表示不要显示提示信息，/S 表示大小写字符敏感方式，/T 表示若在指定的时间内没有选择时，自动执行 /C 中定义的某个选择值。显示文本是 CHOICE 命令执行时的提示信息。选择结果将用 ERRORLEVEL 值来表示。

ECHO：显示指定的信息，通常显示在屏幕上。

如 ECHO Hello 将在屏幕上显示 Hello 的字样。

另外，ECHO ON|OFF 用来设置在批文件执行时是否显示命令本身。而 ECHO OFF 与 @ 的意思一样，但它是一个单独的命令，而不能像 @ 那样放在其他命令之前。

FOR：对于指定的文件运行相应的命令。

在 DOS 下许多命令都支持通配符，如 ? 和 *，可以一次指定一批文件，非常方便。然而，并非所有的 DOS 命令都支持通配符，如 TYPE（文件内容显示命令）就不支持。有了 FOR 命令就没有关系了，利于它可以使 TYPE 命令可以一次显示多个文件。

用法：FOR %变量名 IN（文件集） DO 命令 [命令参数]。

注：以上是 FOR 命令的固定形式，IN 和 DO 的位置必须正确，否则将提示语法错误。

如 FOR %F IN (*.*) DO TYPE %F 命令就可以实现 TYPE 命令一次显示多个文件。

注：%F 是变量名，也可用 %G 等代替，但前后必须一致。在批文件中用 %%F 代替。

GOTO：转到批文件内部的某个标号下执行。

在编程中往往需要重复或跳转到某个地方继续执行，如 BASIC 语言中的 GOTO 命令。批文件中的 GOTO 命令也可以完成类似的功能。

用法：GOTO [标号名]。

其中，标号名是可以随意设置的，如 Hello 等。设置标号用 “:” 符号，如 “: Hello”，这时用 GOTO。

Hello 命令将转到 “:Hello” 所在的位置继续执行批文件。

IF：条件判断命令。这是一项很有用的批处理命令。

用法 1：IF [NOT] EXIST 文件名 命令 [命令参数]。

意义：如果[不]存在某个文件将执行某个命令。

用法 2：IF [NOT] ERRORLEVEL 错误返回代号 命令 [命令参数]。

意义：如果错误返回代号[不]大于或等于指定的代号将执行某个命令。

其中，ERRORLEVEL 表示错误返回代号，很有用。对于很多 DOS 命令，由于执行的结

果不同（如执行成功，执行失败，或被用户中断等），这些命令会返回不同的代号，以表示不同的结果。**ERRORLEVEL** 命令就根据这个不同结果而产生的不同代号来执行不同的命令，通常用在某条命令之后，如 **IF ERRORLEVEL 1 ECHO**。

OK!表示如果当前的错误返回代号大于或等于 1 时将在屏幕上显示“OK!”的字样。

用法 3: **IF [NOT] 字符串 1==字符串 2 命令 [命令参数]**。

意义：当字符串 1 和字符串 2[不]相等的时候执行某个命令。

PAUSE：暂停批文件的执行，并显示“按任意键继续”的字样。

REM：添加注解。用于增加文件可读性，将不被执行。也可以用::来代替。

SHIFT：在批文件中改变可替换参数的位置。

可替换参数是一种特殊的参数，只能用在批文件中。这些参数是由使用者在执行批处理命令时输入的。比如，执行 **DIR /S /W** 命令，其中 **DIR** 是命令名，**/S** 和 **/W** 是它的执行参数。在批文件中，这些命令参数将被分别赋予到可替换参数中，如 **/S** 就成了 %1，**/W** 就成了 %2，以此类推，而命令本身则被赋予 %0 中。批文件就是利用可替换参数对执行时输入的参数来进行操作的。比如现在有个批处理文件叫 **MYFILE.BAT**，在命令行下执行 **MYFILE.BAT YES**，于是 %0 的值就是 **MYFILE.BAT**，%1 的值就是“YES”，可以在此批处理文件中用 **IF** 等命令判断出 %1 等参数的值，然后根据这些值的不同执行不同的操作，如 **IF "%1"=="YES" GOTO YES**。

SHIFT 命令不带任何参数，执行结果是将 %0 的值换成原 %1 的值，而原 %1 的值变成的原 %2 的值，以此类推。注意它的不可逆转性。因为批处理文件执行时的运行参数可能很多，可能会超过 10 个，而可替换参数只能从 %0~%9，若想取得 %9 以后的参数值，只能使用 **SHIFT** 命令。这时，整个参数列将向前推。

以上是 DOS 的自带批处理命令，可以看出，这些命令是非常少的，若要编写较复杂的程序，用以上的命令显然不可能实现。这时就需要其他实用的批处理工具了，著名且实用的有 **TESTIF**，**STRING**，**ASET**，**BATCHMAN**，**WBAT** 等，均可在“DOS 软件分类下载”中的“脚本工具”中下载。在批处理文件中使用以上的工具可以实现非常强大的功能，甚至可以完成许多高级语言程序的功能。所以，如果读者想编写批处理文件时，它们是不错的选择，不仅有详细的文档，而且还在不断发展中。

下面就介绍批处理文件的制作了。其实制作批处理文件并不难，只要掌握了方法就行了。随着你操作次数的增多，你会觉得越来越容易的。

首先使用一个文本编辑器，如 DOS 自带的 **EDIT** 命令或其他的编辑工具，如 **PEDIT** 等新建一个空白文件（当然，用 **COPY CON** 命令直接创建也行），然后在其中根据你想完成的功能输入批处理命令。如果你只是想执行一些 DOS 命令的集合，则按顺序在每行输入一个 DOS 命令就行了。但如果你是想完成一些更复杂的操作，就需要以上的批处理命令或上述的批处理工具了。

以下是作者所编的一个从 1%慢慢增加到 100%的批处理小程序，读者可以做参考，以编写自己的程序。

```
@echo off
break off
cls
set c=0
writext 10 1 Wait...
```

网管天下 网管经验谈

```
be delay 4
:loop
writext 10 9 %c%% completed.
count c
if not %c==101 goto loop
echo.
set c=
kpush /f
break on
```

这里用到了 WRITEXT, COUNT, BE 和 KPUSH, 这些都是批处理工具。WRITEXT 是 ECHO 的增强工具，可以自定义显示的效果。COUNT 是变量的计算工具，如原来 C 的值为 1，执行 COUNT 命令，C 的值就为 2。BE 是个强大的批处理增强工具，在 Norton Utilities 8.0 中带有，KPUSH 是键盘缓冲工具。

总之，利用批处理命令和批处理增强工具，可以编出许多强大的批处理文件来，读者不妨一试。许多批处理工具可以在“脚本工具”中下载。

其实在 DOS 下的一些命令是 Windows 下无可比拟的，首先介绍几个 DOS 下的命令：

(1) delete (DEL)。它能删除在 Windows 下无法删除的文件。比如：Win386.swp（虚拟内存），定期删除可减少硬盘碎片，删除后重启自动可生成 Win386.swp。然而在 Windows 下用鼠标左键单击选定，按键盘上的 Delete 键，弹出确认对话框，确实要把“Win386.swp”放入回收站吗？单击“确定”按钮。又弹出一错误框，无法删除 WIN386：访问被拒绝，请确定磁盘未写保护或未被写保护，而且文件未被使用。

(2) doskey(锁定命令)。在 DOS 下输入如下命令 C:doskey FORMAT=Bad Command or file name!，并按 Enter 键就可以了，当“病毒”或“人毒”格式化你的硬盘时，系统将会显示：“Bad command or file name!”。那么你又问：我自己想格式化时怎么办？没关系！只要输入“C:doskey FORMAT=”并按 Enter 键，就可以了。

(3) FC（它是比较两个文件差别的命令）。命令格式：fc 原文件名 目标文件名 保存结果。例：fc c:1.reg c:2.reg>c:3.txt（其中 1.reg、2.reg 是注册表文件，3.txt 是文本文件），使用这个命令可以比较注册表，也可以比较其他文件（注册表：就是在开始运行并 Enter）。这样在安装共享软件的时候，就知道“它”往注册表中装什么了，（安装前先导出注册表，安装后再导出注册表，并用 FC 命令比较）。

(4) bat（批处理命令），它在 Windows 下同样有它的功效。有一些读者是不是在上网的时候，经常忘了开防火墙，如果在启动 Windows 时直接启动，浪费了系统资源，并不是每次都上网；如果忘了开防火墙，病毒、木马就乘虚而入了，作者本人也有一次教训，能不能两全齐美呢？只要当上网时防火墙自动打开（有一些软件能使两个软件捆绑在一起，只要启动一个软件，另一个软件自动启动），以本人把天网防火墙和电子邮件捆绑一起为例，首先新建记事本（文本文件）内容如下：

```
start C:\Program Files\Skynet\Firewall\snfw.exe
start C:\Program Files\Outlook\1.EXEMSIMN.exe
```

然后另存为（菜单栏中文件另存为）电子邮件.bat（名字随便起，只要后缀是.bat 就行了）然后执行一下，确定是不是成功了。以后收发电子邮件，只要启动这个批处理文件就可以了（也

网管员业余管理经验 | 4

可在桌面或任务栏建立快捷方式，是不是更方便了）。这里需要指出的是：DOS 下不支持长文件名，最多 8 个字节，所以 Program Files 应写成 Progra~1。命令格式即为 start 文件存放路径。

经常使用 DOS，作者总结了几条小技巧，跟读者分享一下：

（1）批处理中用 set 设置 dir 的显示方式。

在批处理命令中加上 c: setdircmd =w/p/a,（三个参数可单独使用）这样只需输入 c: dir, 就可达到分屏五行显示，同时显示隐含目录与文件的效果。若想取消此显示方式，只需输入 c: setdircmd =<-（<- 代表 Enter=同理使用 set 还可以使其他命令简化。

（2）DOS 下 edit 的使用技巧。

使用过 wps 的人都觉得其中“定义块”的功能很好用，其实 DOS 下的 edit 也能实现定义块，并且还有快捷键可使用。先按住 shift 键，再用 → / ← 方向键控制，shift+home 定义到行首，shift+end 定义到行尾，shift+↑ / ↓ 定义上一行和下一行，shift+home+ctrl 定义到文件头……（定义好的块会形成亮带）要想复制块，则首先要定义好块，然后按 Alt+E 组合键，选择 edit 用 ↑ / ↓ 调到 copy 项，按 Enter 键，将定义好的被复制项放到剪贴板中。再将光标移动至目标的位置，按 Alt+E 组合键，选择 paste（粘贴），按 Enter 键，刚刚被放至剪贴板的块被复制到当前光标所在处，移动块也可照此方法。

（3）用 Type 命令复制加密盘。

用 DOS 下的 Type 命令可以复制某些用 copy 及 ptools 无法复制的加密盘上的信息，方法是，先记下目标盘上所有文件的文件名的扩展名，然后在 A: 驱插入源盘，B: 驱插入一张空盘，输入以下命令：A: Type 文件名>B: 文件名，将加密盘上的所有文件按此格式都 Type 到目标盘上，就形成一张与原加密盘一样的盘了。

（4）Type 的另一妙用——获得未知病毒代码。

用 Type 可以巧妙的利用病毒感染 com 和 exe 这一特性，获得未知病毒代码。现在 C 盘根目录下建立两个零字节的 Vir 文件，扩展名分别用 com 和 exe，方法如下：c:>type nul >vir.com, c:>type nul >vir.exe，根据病毒侵入的特性，一旦染毒，扩展名为 com 和 exe 的文件的字节数便会增加。所增加的字节便是感染病毒的全部代码，从而进行有针对性的杀毒措施，如将病毒代码取适当的一段复制到一些杀毒软件的 virus.dat 等病毒代码文件中，就可以自己实现对杀毒软件的升级，非常及时。

很多人对 Windows 操作系统下的 DOS 有一种偏见，其实 DOS 在系统维护工作中有着重要的作用。自从微软公司推出 Windows XP 操作系统后，人们热情的投入到 Windows XP 的怀抱中去关注它、了解它、使用它，却很少有人注意到 Windows XP 附带的 DOS 操作环境，实际上 Windows XP 已经增加了部分 DOS 命令的功能，所谓“老树开新花”，下面让我们一道来感受 Windows XP 下 DOS 的功能变化。

命令：DIR，列文件、目录：

增加参数：/C

参数说明：DIR 列文件、目录时显示的文件大小，其数值以千为单位进行分隔，使用此参数即“DIR/C”将取消显示中的分隔符，以满足部分人的视觉习惯。

增加参数：/Q

参数说明：Windows 是多用户操作系统，使用此参数即“DIR /Q”列文件、目录时，将显示出文件、目录的用户属性。

网管天下 网管经验谈

增加参数：/T:C、/T:A、/T:W

参数说明：使用此参数即“DIR/T:C”、“DIR/T:A”、“DIR/T:W”分别显示文件、目录的创建时间、上次访问时间和上次修改时间。

增加参数：/X

参数说明：使用此参数即“DIR/X”列文件、目录时，会对长文件名同时显示“8.3”格式的文件名。

命令：CD，改变目录：

增加参数：/D

参数说明：此参数的作用是快速改变当前目录，比如当前目录是 C:Windows，使用命令“CD/D E:Tools”可快速切换到 E:Tools 目录下。

注：只有在 Win XP 的“运行”文本框中输入“CMD”得到的 DOS 窗口中才能使用此参数。

命令：MD，建立目录：

功能说明：此命令并未增加参数，但是增强了功能，它可一次建立多级子目录，例如使用命令“MD AABBCDD”将一次性创建 AA、BB、CC、DD 四级子目录。而在老版本的 DOS 中，若不存在 AA 子目录，便无法直接建立 AA 下的 BB 等深层子目录。

命令：RD，删除目录：

增加参数：/S

参数说明：使用此参数即“RD/S”用于删除目录树，即删除目录及目录下的所有子目录和文件，相当于以前版本中的 DELTREE 命令。

增加参数：/Q

参数说明：使用上面的/S 参数删除目录树时，系统会要求用户确认是否真的要删除。若同时使用/Q 参数即“RD/S /Q”，在进行删除操作时将取消确认，相当于 DELTREE 命令的/Y 参数。

命令：DEL，删除文件或目录：

增加参数：/F

参数说明：使用此参数即“DEL/F”可删除只读文件。

增加参数：/S、/Q

参数说明：使用此参数即“DEL/S”作用与“RD/S”完全相同，即删除目录及目录下的所有子目录和文件。同时使用参数/Q，可取消删除操作时的系统确认。

增加参数：/A

参数说明：删除指定属性或指定属性以外的文件，/AR、/AH、/AS、/AA 分别表示删除只读、隐藏、系统、存档文件，/A-R、/A-H、/A-S、/A-A 表示删除除只读、隐藏、系统、存档以外的文件。例如“DEL/AR *.*”表示删除当前目录下所有只读文件，“DEL/A-S *.*”表示删除当前目录下除系统文件以外的所有文件。

命令：ATTRIB，更改文件或目录的属性：

增加参数：/D

参数说明：在 Win XP 中我们不能把文件或文件夹设置为系统属性，只能设为只读、隐藏或存档属性。而带参数/D 使用 ATTRIB 命令可以对文件的所有属性进行设定，设定时必须与参数/S 同时使用。例如“ATTRIB /S /D +S D:Study”，作用是将 D:Study 文件夹设置为系统文

件夹。

命令：format，格式化磁盘：

增加参数：/FS:filesystem

参数说明：按指定文件系统类型（FAT、FAT3（2） NTFS）格式化磁盘，例如“format /FS:NTFS”。

命令：DATE、TIME，显示系统日期和时间：

增加参数：/T

参数说明：使用此参数即“DATE/T”、“TIME/T”将只显示当前日期和时间，而不必输入新日期和时间。

“CD [/D] [drive:][path]

CD [..]”

指定要改成父目录。

输入 CD 驱动器，显示指定驱动器中的当前目录。

不带参数只输入 CD，则显示当前驱动器和目录。

使用/D 命令行开关，除了改变驱动器的当前目录之外，还可改变当前驱动器。

CHDIR 命令不把空格做分隔符，因此有可能将目录名改为一个。带有空格但不带有引号的子目录名。例如：

```
cd winntprofilesusernameprogramsstart menu
```

与下列相同

```
cd "winntprofilesusernameprogramsstart menu"
```

在扩展功能停用的情况下，你必须输入以上命令。

COPY:将一份或多份文件复制到另一个位置。

```
COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/A | /B ] source [/A | /B]  
[+ source [/A | /B] [+ ...]] [destination [/A | /B]]
```

source 指定要复制的文件。

/A 表示一个 ASCII 文本文件。

/B 表示一个二进位文件。

/D 允许解密要创建的目标文件

destination 为新文件指定目录和/或文件名。

/V 验证新文件写入是否正确。

/N 复制带有非 8dot3 名称的文件时，尽可能使用短文件名。

/Y 不使用确认是否要改写现有目标文件的提示。

/-Y 使用确认是否要改写现有目标文件的提示。

/Z 用可重新启动模式复制已联网的文件。命令行开关/Y 可以在 COPYCMD 环境变量中预先设定。这可能会被命令行上的/-Y 替代。除非 COPY 命令是在一个批文件脚本中执行的，默认值应为在改写时进行提示。

要附加文件，请为目标指定一个文件，为源指定数个文件（用通配符或 file1+file2+file3 格式）。

网管天下 网管经验谈

DATE:显示或设置日期。

```
DATE [/T | date]
```

显示当前日期设置和输入新日期的提示，请输入不带参数的 **DATE**。要保留现有日期，请按 **ENTER** 键。

如果命令扩展名被启用，**DATE** 命令会支持 **/T**。

开关该开关指示命令只输出当前日期，但不提示输出新日期。

DEL:删除一个或数个文件。

```
DEL [/P] [/F] [/S] [/Q] [/A[:attributes]] names  
ERASE [/P] [/F] [/S] [/Q] [/A[:attributes]] names
```

names 指定一个或数个文件或目录列表。通配符可被用来删除多个文件。如果指定了一个目录，目录中的所有文件都会被删除。

/P 删除每一个文件之前提示确认。

/F 强制删除只读文件。

/S 从所有子目录删除指定文件。

/Q 安静模式。删除全局通配符时，不要求确认。

/A 根据属性选择要删除的文件。

attributes **R** 只读文件 **S** 系统文件 **H** 隐藏文件 **A** 存档文件。

如果命令扩展名被启用，**DEL** 和 **ERASE** 会如下改变：

S 开关的显示句法会颠倒，即只显示已经删除的文件，而不显示找不到的文件。

```
DIR [drive:][path][filename] [/A[:attributes]] [/B] [/C] [/D] [/L] [/N]  
[/O[:sortorder]] [/P] [/Q] [/S] [/T[:timefield]] [/W] [/X] [/4]  
[drive:][path][filename]
```

指定要列出的驱动器、目录和/或文件。

/A 显示具有指定属性的文件。

attributes **D** 目录 **R** 只读文件 **H** 隐藏文件 **A** 准备存档的文件 **S** 系统文件 - 表示“否”的前缀。

/B 使用空格式（没有标题信息或摘要）。

/C 在文件大小中显示千位数分隔符。这是默认值。用 **/-C** 来停用分隔符显示。

/D 跟宽式相同，但文件是按栏分类列出的。

/L 用小写。

/N 新的长列表格式，其中文件名在最右边。

/O 用分类顺序列出文件。

sortorder **N** 按名称（字母顺序） **S** 按大小（从小到大） **E** 按扩展名（字母顺序） **D** 按日期/时间（从先到后） **G** 组目录优先 - 颠倒顺序的前缀。

/P 在每个信息屏幕后暂停。

/Q 显示文件所有者。

/S 显示指定目录和所有子目录中的文件。

/T 控制显示或用来分类的时间字符域。

timefield C 创建时间 **A** 上次访问时间 **W** 上次写入的时间。

/W 用宽列表格式。

/X 显示为非 8dot3 文件名产生的短名称。格式是 **/N** 的格式，短名称插在长名称前面。

如果没有短名称，在其位置则显示空白。

可以在 **DIRCMD** 环境变量中预先设定开关。通过添加前缀 **-**（破折号）来替代预先设定的开关。例如，**/-W**。

DISKCOMP:比较两张软盘的内容。

```
DISKCOMP [drive1: [drive2:]]
```

DISKCOPY:把一张软盘的内容复制到另一张。

```
DISKCOPY [drive1: [drive2:]] [/V]
```

/V 校验信息复制的是否正确。

两张软盘的类型必须相同。

你可以为 **drive1** 和 **drive2** 指定同样的驱动器。

ECHO:显示信息，或将命令回显打开或关上。

```
ECHO [ON | OFF]
```

```
ECHO [message]
```

要显示当前回显设置，输入不带参数的 **ECHO**。

FC:比较两个文件或两个文件集并显示它们之间的不同

```
FC [/A] [/C] [/L] [/LBn] [/N] [/OFF[LINE]] [/T] [/U] [/W] [/nnnn]
```

```
[drive1:][path1]filename1 [drive2:][path2]filename2
```

```
FC /B [drive1:][path1]filename1 [drive2:][path2]filename2
```

/A 只显示每个不同处的第一行和最后一行。

/B 执行二进制比较。

/C 不分大小写。

/L 将文件作为 ASCII 文字比较。

/LBn 将连续不匹配的最大值设为指定的行数。

/N 在 ASCII 比较上显示行数。

/OFF[LINE] 不要跳过带有脱机属性集的文件。

/T 不要将 **tab** 扩充到空格。

/U 将文件作为 UNICODE 文字文件比较。

/W 为了比较而压缩空白（**tab** 和空格）。

/nnnn 指定不匹配处后必须连续匹配的行数。

"[drive1:][path1]filename1"。

指定要比较的第一个文件或第一个文件集。

"[drive2:][path2]filename2"。

指定要比较的第二个文件或第二个文件集。

FIND:在文件中搜索字符串。

网管天下 网管经验谈

```
"FIND [/V] [/C] [/N] [/I] [/OFF[LINE]] "string" [[drive:][path]filename[...]]"
```

/V 显示所有未包含指定字符串的行。

/C 仅显示包含字符串的行数。

/N 显示行号。

/I 搜索字符串时忽略大小写。

/OFF[LINE] 不要跳过具有脱机属性集的文件。

FORMAT:格式化磁盘。

```
FORMAT volume [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/X]
FORMAT volume [/V:label] [/Q] [/F:size]
FORMAT volume [/V:label] [/Q] [/T:tracks /N:sectors]
FORMAT volume [/V:label] [/Q]
FORMAT volume [/Q]
```

volume 指定驱动器（后面跟一个冒号）、装入点或卷名。

/FS:filesystem 指定文件系统类型（FAT、FAT32 或 NTFS）。

/V:label 指定卷标。

/Q 执行快速格式化。

/C 仅适于 NTFS: 默认情况下，将压缩在该新建卷上创建的文件。

/X 如果必要，先强制卸下卷。那时，该卷所有打开的句柄不再有效。

/A:size 替代默认配置单位大小。极力建议你在一般状况下使用默认设置。

NTFS 支持 51(2) 102(4) 204(8) 409(6) 819(2) 16 KB、32 KB、64 KB。

FAT 支持 51(2) 102(4) 204(8) 409(6) 819(2) 16 KB、32 KB、64 KB、(128 KB、256 KB 用于大于 512 字节的扇区)。

FAT32 支持 51(2) 102(4) 204(8) 409(6) 819(2) 16 KB、32 KB、64 KB、(128 KB、256 KB 用于大于 512 字节的扇区)。

注意 FAT 及 FAT32 文件系统对卷上的群集数量有以下限制。

FAT: 群集数量 ≤ 65526 。

FAT32: $65526 < \text{群集数量} < 4177918$ 。

如果判定使用指定的群集大小无法满足以上需求，格式化将立即停止。

NTFS 压缩不支持大于 4096 的分配单元。

/F:size 指定要格式化的软盘大小（1.44）。

/T:tracks 为磁盘指定每面磁道数。

/N:sectors 指定每条磁道的扇区数。

LABEL:创建、更改或删除磁盘的卷标。

```
LABEL [drive:][label]
LABEL [/MP] [volume] [label]
```

drive: 指定驱动器名。

label 指定卷标签。

/MP 指定卷应该被当做安装点或卷名。

volume 指定驱动器（后面跟一个冒号）、装入点或卷名。如果指定了卷名，/MP 标志则

不必要。

MD:创建目录:

```
MKDIR [drive:]path
MD [drive:]path
```

要移动至少一个文件:

```
MOVE [/Y | /-Y] [drive:][path]filename1[,...] destination
```

要重命名一个目录:

```
MOVE [/Y | /-Y] [drive:][path]dirname1 dirname2
[drive:][path]filename1
```

指定你想移动的文件位置和名称。

destination 指定文件的新位置。目标可包含一个驱动器号和冒号、一个目录名或组合。如果只移动一个文件并在移动时将其重命名，你还可以包括文件名。

```
[drive:][path]dirname1
```

指定要重命名的目录。**dirname2** 指定目录的新名称。

/Y 取消确认改写一个现有目标文件的提示。

/-Y 对确认改写一个现有目标文件发出提示。

命令行开关 **/Y** 可以出现在 **COPYCMD** 环境变量中。这可以用命令行上的 **/-Y** 替代。

除非 **MOVE** 命令是从一个批脚本内执行的，改写时都发出提示。

PROMPT:更改命令提示符。

```
PROMPT [text]
```

text 指定新的命令提示符。

提示符可以由普通字符及下列特定代码组成:

& (短 **and** 符号)

| (管道)

((左括弧)

当前日期

Escape code (ASCII 码 27)

) (右括弧)

> (大于符号)

Backspace (擦除前一个字符)

< (小于符号)

当前驱动器

当前驱动器及路径

= (等号)

(空格)

当前时间

网管天下 网管经验谈

版本号

/usr/local/apache/bin/httpd 换行

\$\$\$（货币符号）

如果命令扩展名被启用，PROMPT 命令会支持下列格式化字符：

\$+ 根据 PUSHd 目录堆栈的深度，零个或零个以上加号（+）字符；

每个被推的层有一个字符。

如果当前驱动器不是网络驱动器，显示跟当前驱动器号或

空字符串有关联的远程名。

TIME:显示或设置系统时间。

“TIME [T | time]”

显示当前时间设置和输入新时间的提示，请输入不带参数的 TIME。要保留现有时间，请按 ENTER 键。

如果命令扩展名被启用，DATE 命令会支持 /T 命令行开关；该命令行开关告诉命令只输出当前时间，但不提示输出新时间。

TREE:以图形显示驱动器或路径的文件夹结构。

TREE [drive:][path] [/F] [/A]

/F 显示每个文件夹中文件的名称。

/A 使用 ASCII 字符，而不使用扩展字符。

VER:显示 DOS / Windows 版本。

XCOPY:复制文件和目录树。

```
XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
[/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]
[/K] [/N] [/O] [/X] [/Y] [/Y] [/Z]
[/EXCLUDE:file1[+file2][+file3]...]
```

source 指定要复制的文件。

destination 指定新文件的位置和/或名称。

/A 只复制有存档属性集的文件，但不改变属性。

/M 只复制有存档属性集的文件，并关闭存档属性。

/D:m-d-y 复制在指定日期或指定日期以后改变的文件。如果没有提供日期，只复制那些源时间比目标时间新的文件。

/EXCLUDE:file1[+file2][+file3]...

指定含有字符串的文件列表。如果有任何字符串与要被复制的文件的绝对路径相符，那文件将不会得到复制。

例如，指定如 obj 或 .obj 的字符串会排除

目录 obj 下面的所有文件或带有

.obj 扩展名的文件。

/P 创建每个目标文件前提示。

/S 复制目录和子目录，除了空的。

/E 复制目录和子目录，包括空的。

与 /S /E 相同。可以用来修改 /T。

/V 验证每个新文件。
/W 提示你在复制前按键。
/C 即使有错误，也继续复制。
/I 如果目标不存在，又在复制一个以上的文件，假定目标一定是一个目录。
/Q 复制时不显示文件名。
/F 复制时显示完整的源和目标文件名。
/L 显示要复制的文件。
/G 允许将没有经过加密的文件复制到不支持加密的目标。
/H 也复制隐藏和系统文件。
/R 改写只读文件。
/T 创建目录结构，但不复制文件。不包括空目录或子目录。/T /E 包括空目录和子目录。

/U 只复制已经存在于目标中的文件。
/K 复制属性。一般的 Xcopy 会重设只读属性。
/N 用生成的短名复制。
/O 复制文件所有权和 ACL 信息。
/X 复制文件审核设置（隐含 /O）。
/Y 禁止提示以确认改写一个现存目标文件。
/Y 导致提示以确认改写一个现存目标文件。
/Z 用重新启动模式复制网络文件。

使用批处理文件——常用命令

echo、@、call、pause、rem 是批处理文件最常用的几个命令，echo 表示显示此命令后的字符，echo off 表示在此语句后所有运行的命令都不显示命令行本身。@与 echo off 相同，但它是加在其他命令行的最前面，表示运行时不显示命令行本身。

call 调用另一条批处理文件（如果直接调用别的批处理文件，执行完一条文件后将无法执行当前文件后续命令）

pause 运行此句会暂停，显示“Press any key to continue...”等待用户按任意键后继续。

rem 表示此命令后的字符为解释行，不执行，只是给自己今后查找用的。

例：用 edit 编辑 a.bat 文件，输入下列内容后存盘为 c:a.bat，执行该批处理文件后可实现。
将根目录中所有文件写入 a.txt 中，启动 UCDOS，进入 WPS 等功能。

批处理文件的内容为：echo off 不显示命令行

dir c:*. * >a.txt 将 c 盘文件列表写入 a.txt

call c:ucdosucdos.bat 调用 ucdos

echo 你好，显示"你好"

pause 暂停，等待按键继续

rem 使用 wps 注释将使用 wps

cd ucdos 进入 ucdos 目录

wps 使用 wps

批处理文件中还可以像 C 语言一样使用参数，这只需用到一个参数表示符%。

%表示参数，参数是指在运行批处理文件时在文件名后加的字符串。变量可以从%0~%9，

网管天下 网管经验谈

%0 表示文件名本身，字符串用%1~%9 顺序表示。

例如，C：根目录下一批处理文件名为 f.bat，内容为 format %1 即执行 C:>f a:可实际执行的是 format a: 又如 C：根目录下一批处理文件的名为 t.bat，内容为 type %1 type %2 那么运行 C:>t a.txt b.txt，将顺序地显示 a.txt 和 b.txt 文件的内容。

if goto choice for 是批处理文件中比较高级的命令。

if 表示将判断是否符合规定的条件，从而决定执行不同的命令，有 3 种格式：

(1) if "参数"=="字符串"待执行的命令。

参数如果等于指定的字符串，则条件成立，运行命令，否则运行下一句。（注意是两个等号）

如 if "%1"=="a" format a:

(2) if exist 文件名 待执行的命令。

如果有指定的文件，则条件成立，运行命令，否则运行下一句。如 if exist config.sys edit config.sys

(3) if errorlevel 数字待执行的命令。

如果返回码等于指定的数字，则条件成立，运行命令，否则运行下一句。如 if errorlevel 2 goto x2 DOS 程序运行时都会返回一个数字给 DOS，称为错误码 errorlevel 或称返回码。goto 批处理文件运行到这里将跳到 goto 所指定的标号处，一般与 if 配合使用。如：

“goto end

end

echo this is the end”

标号用 :字符串表示，标号所在行不被执行。

choice 使用此命令可以让用户输入一个字符，从而运行不同的命令。使用时应该加/c:参数，c:后应写提示可输入的字符，之间无空格。它的返回码为 1234……

如：choice /cme defrag,mem,end

将显示

```
defrag,mem,end[D,M,E]?
```

例如，test.bat 的内容如下：

```
@echo off
choice /cme defrag,mem,end
if errorlevel 3 goto defrag 应先判断数值最高的错误码
if errorlevel 2 goto mem
if errorlevel 1 goto end
efrag
c:dosdefrag
goto end
mem
mem
goto end
end
echo good bye "
```

网管员业余管理经验 | 4

此文件运行后，将显示 defrag,mem,end[D,M,E]? 用户可选择 d m e，然后 if 语句将做出判断，d 表示执行标号为 defrag 的程序段，m 表示执行标号为 mem 的程序段，e 表示执行标号为 end 的程序段，每个程序段最后都以 goto end 将程序跳到 end 标号处，然后程序将显示 good bye，文件结束。

for 循环命令，只要条件符合，它将多次执行同一命令。

格式 FOR [%%f] in (集合) DO [命令]。

只要参数 f 在指定的集合内，则条件成立，执行命令。

如果一条批处理文件中有一行：“for %%c in (*.bat *.txt) do type %%c”，其含义是如果以 bat 或 txt 结尾的文件，则显示文件的内容。

DOS 在启动时会自动运行 autoexec.bat 这条文件，一般我们在里面装载每次必用的程序，如：path（设置路径）、smartdrv（磁盘加速）、mouse（鼠标启动）、mscdex（光驱连接）、doskey（键盘管理）、set（设置环境变量）等。

如果启动盘根目录中没有这个文件，计算机会让用户输入日期和时间。

例如，一个典型的 autoexec.bat 内容如下：

```
@echo off 不显示命令行
prompt
path c:dos;c:;c:windows;c:ucdos;c:tools 设置路径
lh c:dosdoskey.com 加载键盘管理
lh c:mousemouse.com 加载鼠标管理
lh c:dossmartdrv.exe 加载磁盘加速管理
lh c:dosmscdex /S /D:MSCD000 /M:12 /V 加载 CD-ROM 驱动
set temp=c:temp 设置临时目录
```

10.for 命令

for 命令是一个比较复杂的命令，主要用于参数在指定的范围内循环执行命令。在批处理文件中使用 FOR 命令时，指定变量请使用

```
%%variable
for {%variable|%%variable} in (set) do command [ CommandLineOptions]
```

%variable 指定一个单一字母可替换的参数。

(set) 指定一个或一组文件。可以使用通配符。

command 指定对每个文件执行的命令。

command-parameters 为特定命令指定参数或命令行开关。

在批处理文件中使用 FOR 命令时，指定变量请使用 %%variable 而不要用 %variable。

变量名称是区分大小写的，所以 %i 不同于 %I。

如果命令扩展名被启用，下列额外的 FOR 命令格式会受到支持。

```
FOR /D %variable IN (set) DO command [command-parameters]
```

如果集中包含通配符，则指定与目录名匹配，而不与文件名匹配。

```
FOR /R [[drive:]path] %variable IN (set) DO command [command]
```

检查以 [drive:]path 为根的目录树，指向每个目录中的 FOR 语句。如果在 /R 后没有指

网管天下 网管经验谈

定目录，则使用当前目录。如果集仅为一个单点（.）字符，则枚举该目录树。

```
FOR /L %variable IN (start,step,end) DO command [command-para]
```

该集表示以增量形式从开始到结束的一个数字序列。

因此，(1,1,5) 将产生序列 1 2 3 4 5，(5,-1,1) 将产生序列 (5 4 3 2 1)。

```
FOR /F ["options"] %variable IN (file-set) DO command
FOR /F ["options"] %variable IN ("string") DO command
FOR /F ["options"] %variable IN ('command') DO command
```

或者，如果有 usebackq 选项：

```
FOR /F ["options"] %variable IN (file-set) DO command
FOR /F ["options"] %variable IN ("string") DO command
FOR /F ["options"] %variable IN ('command') DO command
```

filenameset 为一个或多个文件名。继续到 filenameset 中的下一个文件之前，每份文件都已被打开、读取并经过处理。处理包括读取文件，将其分成一行行的文字，然后将每行解析成零或更多的符号。然后用已找到的符号字符串变量值调用 For 循环。以默认方式，/F 通过每个文件的每一行中分开的第一个空白符号。跳过空白行。你可通过指定可选 "options" 参数替代默认解析操作。这个带引号的字符串包括一个或多个指定不同解析选项的关键字。这些关键字为：eol=c - 指一个行注释字符的结尾（就一个）。

4.1.3 限制上外网的经验

作为网管员，经常因为单位要求而需要限制部分或全部工作人员在上班时上外网。在大多数单位，都是通过限制工作站的 IP 地址，控制其上网行为。例如，根据部门、人员的不同，为其分配不同的地址或者地址段，在防火墙（或代理服务器）中设置上网策略。但这样的设置，存在以下几方面的问题：

(1) 因为知道网管对 IP 地址进行了限制，所以一些员工会将自己的 IP 地址改成不受限制的 IP 地址，以避开限制。这样，经常造成网络地址的冲突。

(2) 为了解决员工随意修改 IP 地址的问题，需要将 IP 地址与 MAC 地址绑定。但这样需要对三层交换机进行调试，并会增加网管的负担。另外，现在修改网卡的 MAC 地址也是非常容易的，这也不是解决问题的最终方法。

(3) 如果只是通过 IP 地址限制上网，由于现在的笔记本电脑很多。如果外来人员将随身携带的笔记本电脑接入网络，设置一个 IP 地址，就可以访问外网，这样也可能引发问题。

(4) 当网络出现问题时，如果只是基于 IP 地址进行排查，不容易定位故障源，因为 IP 地址是可以随意设置的。

为了解决上述问题，本节将介绍联合使用 ISA Server、DHCP、DNS、Windows Server 2003 Active Directory 的综合解决方案，达到让指定的用户、在指定的时间、以指定的流量、访问指定的网络的目的。本方案只对用户身份进行验证，不需对 IP 地址进行限制，即使用户修改 IP 地址，也不能避开限制。本方案网络拓扑如图 4-1 所示。

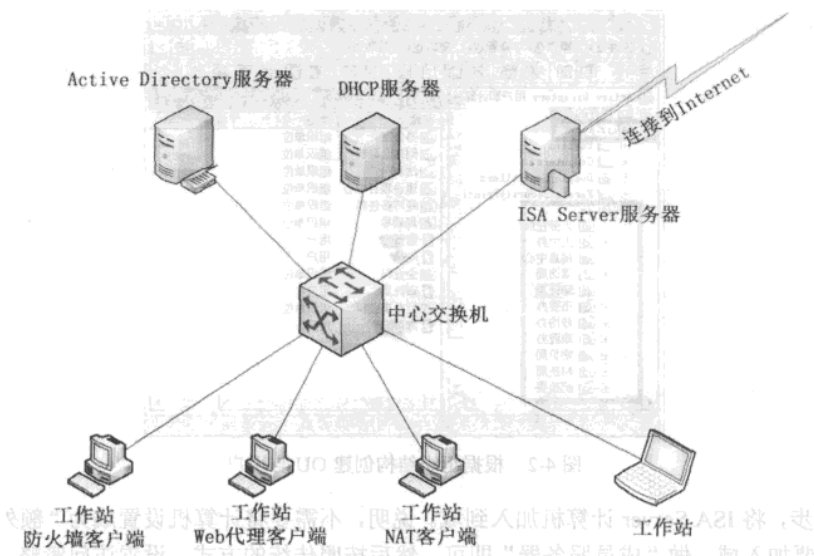


图 4-1 网络拓扑

解决思路如下：

- (1) 在网络中需要有一台 Windows Server 2003 的服务器，升级到 Active Directory（域），用于提供身份验证。所有的工作站需要加入该域，ISA Server 是该域的“成员服务器”。
- (2) 网络中提供一台 DHCP 服务器，为工作站自动分配 TCP/IP 地址（可选）。
- (3) 在 ISA Server 中创建访问策略时，采用“身份验证”方式，没有经过身份验证的计算机不能访问指定的网络（一般是访问 Internet）。
- (4) 因为 ISA Server 2004、ISA Server 2006 没有提供“流量”限制功能，可以采用第三方的“Bandwidth Splitter for Microsoft ISA Server”软件，提供流量限制功能。
- (5) 所有的工作站在访问 Internet 时，需要采用“Web 代理方式”或“ISA Server 的防火墙客户端”，否则不能通过“身份验证”，也就不能访问外网。

为了统一起见，网络中重要服务器的参数如下：

Active Directory 服务器的 IP 地址为 192.168.7.7，ISA Server 服务器的“内网”地址为 10.10.0.1（三层交换机的默认路由所指定的地址），外网地址为 61.182.x.y；DHCP 服务器的地址为 192.168.7.6（三层交换机中设置“DHCP 中继代理的”地址）。所有的工作站采用 192.168.1.0/24~192.168.6.0/24 的网段，DNS 地址设置为 192.168.7.7。

在 ISA Server 中，使用“Web 代理客户端”与“防火墙客户端”，可以通过身份验证。下面分别介绍一下这两种客户端的设置方法。

■ 1. 使用 Web 代理客户端上网

第 1 步，在网络中一台 Windows Server 2003 的服务器上，将 DNS 地址设置成 127.0.0.1，运行 dcpromo，将计算机升级到 Active Directory。在本例中，DNS 域名为 jz.local，升级到域之后，按照单位的组织机构创建 OU、子 OU（与部门名称相同），并在子 OU 中创建用户，如图 4-2 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

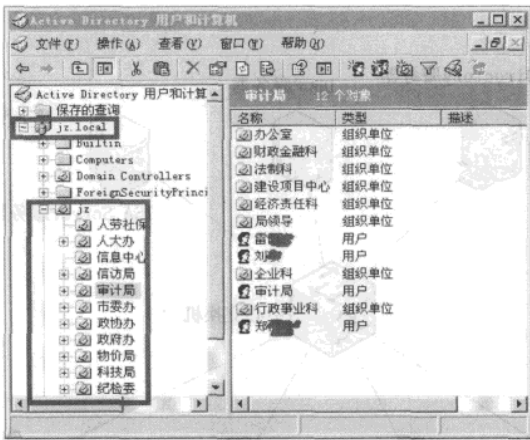


图 4-2 根据组织结构创建 OU 与用户

第 2 步，将 ISA Server 计算机加入到域。说明，不需要将计算机设置成为“额外的域控制器”，只要加入域，做“成员服务器”即可。然后按照传统的方式，设置访问策略，例如“允许内网访问外网”，即在创建规则时，允许“内部”用户访问“外部”，但在设置“用户”时，将默认的“所有用户”删除，而是添加“所有域用户”或者“所有通过身份验证的用户”，如图 4-3 所示。

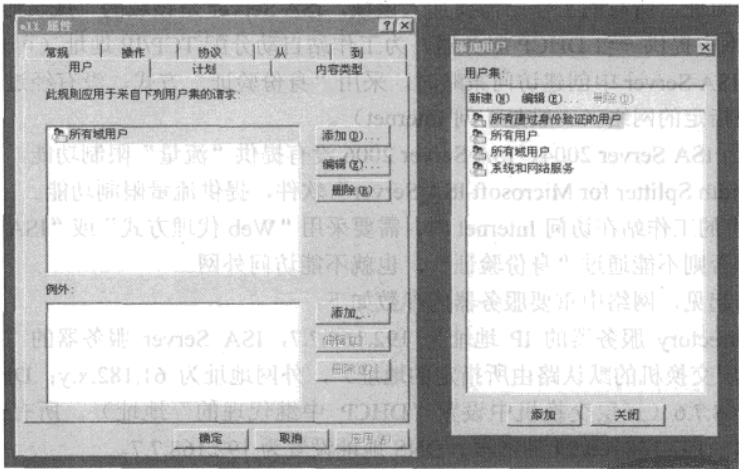


图 4-3 用户规则

这样，原来只根据 IP 地址的限制，变成了 IP 地址+用户身份限制，但在创建策略时，允许所有“内部”的用户，这样，起决定作用的就是“用户身份”了。

第 3 步，在“配置→网络”中，双击“内部”选项，在打开的“内部 属性”页中的“Web 代理”选项卡中，选中“为此网络启用 Web 代理客户端连接”和“启用 HTTP”复选框，如图 4-4 所示。设置策略之后，单击“确定”按钮，让设置生效。

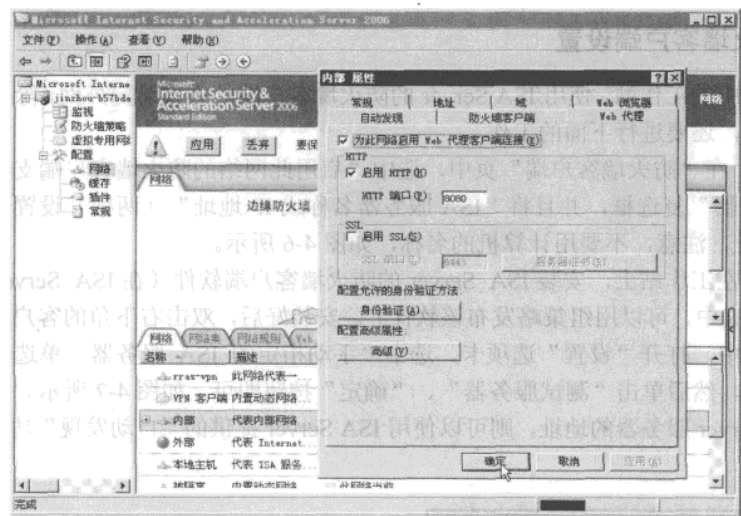


图 4-4 启用 Web 代理并指定代理端口

第 4 步，返回到“Active Directory”服务器上，在“Active Directory 用户和计算机”中，编辑该 OU 所在的策略。在“用户配置→Windows 设置→Internet Explorer 维护→连接”中，双击右侧的“代理设置”选项，在弹出的对话框中，选中“启用代理服务器设置”复选框，在“HTTP”文本框中输入代理服务器的地址（在本例中为 10.10.0.1）与端口（本例中为 8080），如图 4-5 所示。

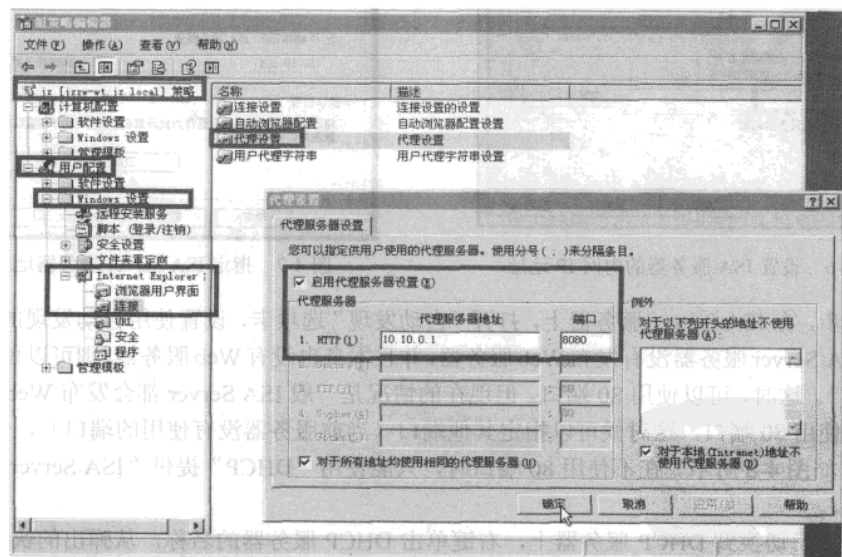


图 4-5 编辑策略

第 5 步，所有的工作站加入到域之后，以域用户登录，其 IE 中的代理服务器地址，将会按照图 4-5 中的进行设置，并且可以访问 Internet。如果没有加入到域，则不能访问 Internet。

2. 防火墙客户端设置

如果网络中的工作站，使用 ISA Server 的防火墙客户端的方式访问外网，除了需要按照上面进行设置外，还要进行下面的工作。

第 1 步，在“防火墙客户端”页中，选中“启用此网络的防火墙客户端支持”与“使用 Web 代理服务器”复选框，并且将“ISA 服务器名称或 IP 地址”（两处）设置为 ISA Server 内网的 IP 地址，注意，不要用计算机的名称，如图 4-6 所示。

第 2 步，在工作站上，安装 ISA Server 的防火墙客户端软件（在 ISA Server 安装光盘的“Client”文件夹中，可以用组策略发布该软件）。安装好后，双击右下角的客户端的图标，在弹出的对话框中，打开“设置”选项卡，选中“手动指定的 ISA 服务器”单选按钮，在其中输入 10.10.0.1，然后单击“测试服务器”、“确定”按钮即可，如图 4-7 所示。如果不想让用户指定 ISA Server 服务器的地址，则可以使用 ISA Server 提供的“自动发现”功能，这需要进行进一步的配置。

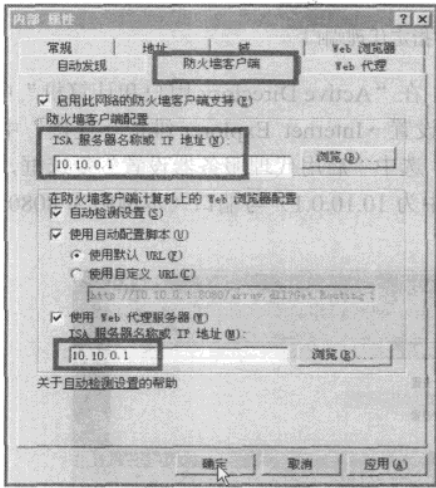


图 4-6 设置 ISA 服务器的内网 IP 地址



图 4-7 指定 ISA Server 服务器地址

第 3 步，在 ISA Server 服务器上，打开“自动发现”选项卡，设置使用自动发现的端口号。如果该 ISA Server 服务器没有发布 Web 服务器，并且本身也没有 Web 服务器，则可以使用“DNS 发现功能”，这时，可以使用 80 端口。但现在的情况是一般 ISA Server 都会发布 Web 服务器，所以不能使用 80 端口，这时候可以指定其他端口（当前服务器没有使用的端口），例如 TCP 的 2501，如图 4-8 所示。在不使用 80 端口时，只能使用“DHCP”提供“ISA Server”的自动发现功能。

第 4 步，切换到 DHCP 服务器上，右键单击 DHCP 服务器的名称，从弹出的快捷菜单中选择“设置预定义的选项”命令，单击“添加”按钮。在“选项类型”对话框中的“名称”处输入大写的 WPAD，“数据类型”选择“字符串”，“代码”选择 252，在“描述”处输入 http://10.10.0.1:2501/wpad.dat，然后单击“确定”按钮，如图 4-9 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

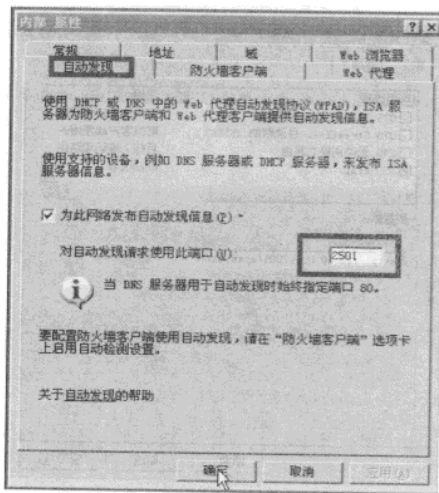


图 4-8 设置 DNS 自动发现

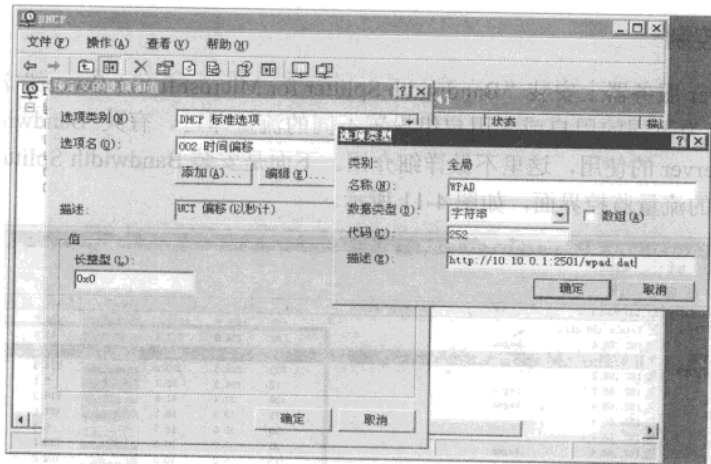


图 4-9 添加 WPAD 选项

添加之后，右键单击“服务器选项”选项，在弹出的“服务器 选项”对话框中，选中添加的“252 WPAD”复选框，如图 4-10 所示。

说·明 还需要为每个 VLAN 创建作用域、设置作用域的地址范围、子网掩码、网关地址，并在“服务器选项”中，添加 DNS 地址为 192.168.7.7，这里不再一一介绍。

经过上述设置后，每台工作站设置“自动获得 IP 地址”与“DNS”地址，同时，ISA Server 的“防火墙客户端”，就可以自动通过 DHCP 的 WPAD 选项，自动指定 ISA Server 服务器的地址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

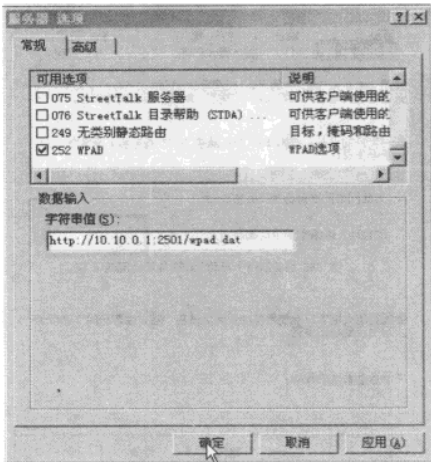


图 4-10 启用 WPAD 选项

3. 流量控制

在 ISA Server 服务器上安装“Bandwidth Splitter for Microsoft ISA Server”流量控制软件，并且设置策略，为不同的用户或者用户组设置不同的流量即可。有关 Bandwidth Splitter for Microsoft ISA Server 的使用，这里不做详细介绍。下面是安装 Bandwidth Splitter for Microsoft ISA Server 之后的流量监控界面，如图 4-11 所示。

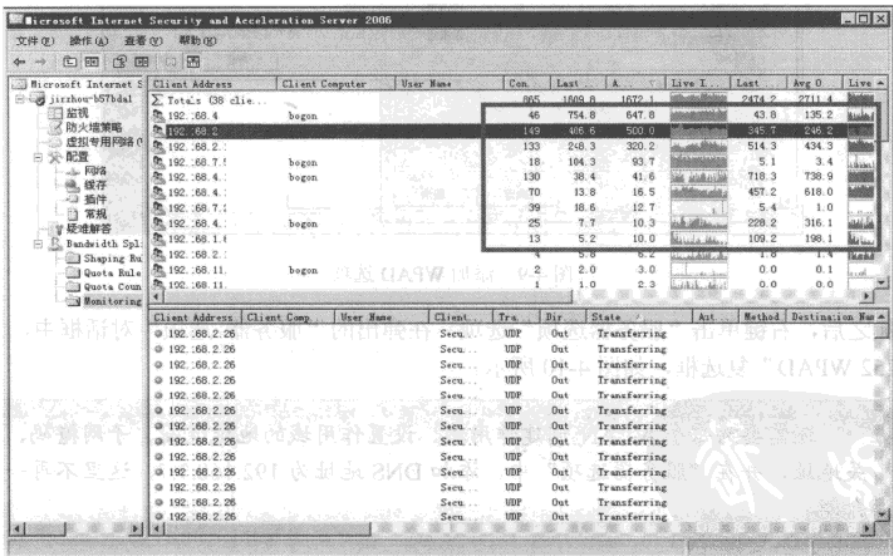


图 4-11 流量监测图

在使用流量限制后（还可以限制并发连接数量），当网络中某人说他的计算机上网慢时，可以在流量控制列表中，根据显示的“用户名”查看该计算机的流量，以及访问的网站。如果

网管员业余管理经验 | 4

网络速度慢是由于该用户下载软件或看视频导致，则提醒该用户。这样，也弥补了 ISA Server 的不足。

4. 其他设置

如果使用 Web 代理客户端或者防火墙客户端的计算机，网络中有服务器，例如一些内部网站服务器，则在访问这些内部网站时，不应该使用代理服务器，这时候，可以在 ISA Server 上进行设置。

在 ISA Server 服务器上的“内部属性”中，选中“直接访问在‘域’选项卡中指定的计算机”和“直接访问‘地址’选项卡中指定的计算机”复选框，或者单击“添加”按钮，将内网服务器的地址添加到“直接访问这些服务器或域”列表中即可，如图 4-12 所示。

最后，如果网络中有服务器、计算机，由于使用 Web 代理客户端或防火墙客户端出现访问网络问题，或者有的服务器只能使用 NAT 的客户端，可以将这些服务器、计算机的 IP 地址创建一个“计算机集”，单独针对这些计算机集创建访问策略，并且这些访问策略要在其他访问策略的前面，这些是 ISA Server 的使用技巧，本节不做过多介绍。

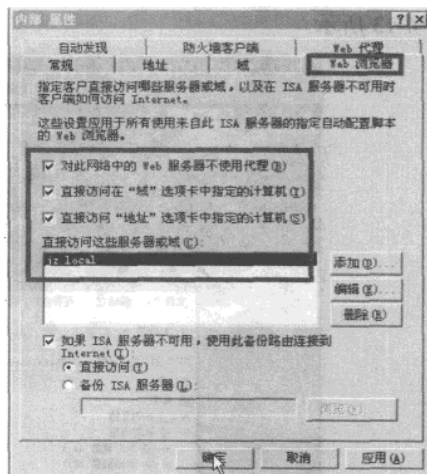


图 4-12 需要直接访问的地址

4.2 网络管理工具使用经验

本节主要介绍了几种网络管理工具的使用经验，利用网络工具进行网络的管理，相信定能使网络管理成为一种比较方便的工作。另外，本节还介绍了利用系统自带的工具进行网络管理的经验。

4.2.1 使用“云端软件平台”的经验

作为网管员的我们对管理软件的热度从未降低过，最近网上看到一款名为“云端软件平台”软件，下载试用了一下，感觉不错，所以本节就向读者介绍一下这款软件。

目标客户：家庭个人用户、一般单位用户，对安装软件感到“头疼”的初学者、愿意尝“鲜”的计算机爱好者。

功能：云端为软件提供虚拟化的运行环境，能够保持系统长久的干净、绿色，为软件虚拟注册表、文件 IO 等，避免了软件安装、使用、卸载带来的系统污染。软件想用就用，不怕垃圾污染；不需要了，一键删除，快速无痕，云端帮你实现全面绿色化。

简单来说，任意一台能上网的计算机，只需要安装“云端软件平台”客户端软件，以后不再需要向以前那样下载（或从其他途径）软件、安装、配置、使用，而只是从“云端软件平

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

台”提供的浏览器下载软件，下载之后即可以使用，免去了用户安装、配置的繁琐手续。

1. 软件的安装主要步骤

(1) 云端软件平台目前为 0.9Beta 版，大小只有 576KB。软件的安装非常简单，只要从 <http://www.yunduan.cn/index.php> 下载软件，直接解压缩展开，运行其中的 cloud.exe 即可，如图 4-13 所示。

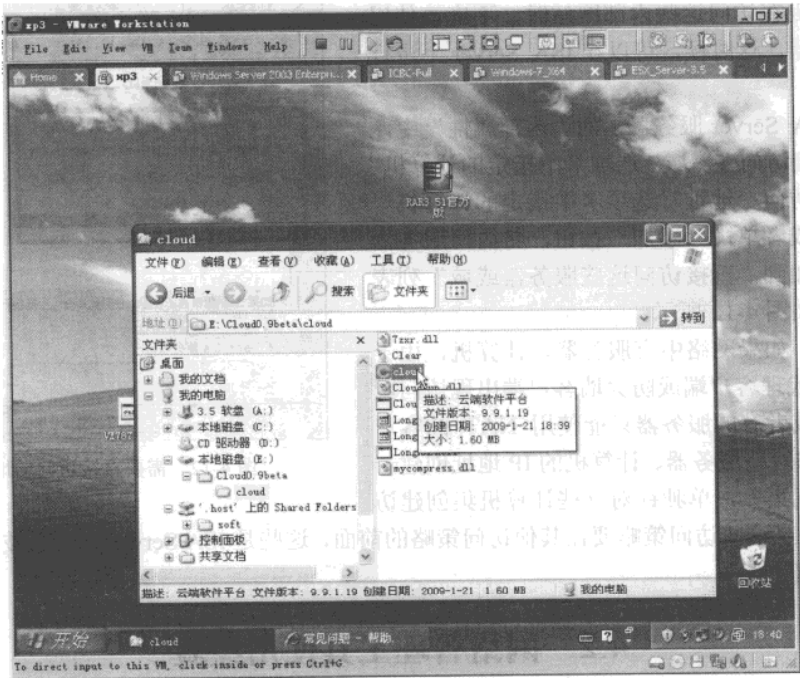


图 4-13 运行 cloud 程序

(2) 在第一次运行的时候，选择一个缓存目录，如图 4-14 所示。

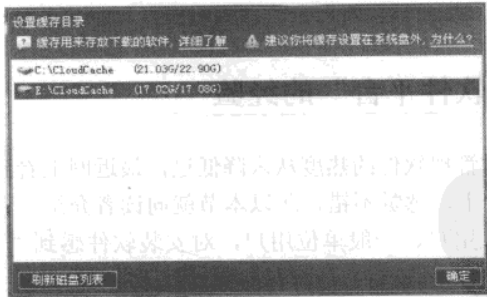


图 4-14 设置缓存目录

2. 下载软件并使用简介

(1) 进入软件界面后，在右侧的“软件库”中，选择要下载并使用的软件，按 Enter 键，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

软件会下载到本地，如图 4-15 所示。在下载每个软件前，可以为软件选择分类（也可以创建之后再选择）。



图 4-15 选择并下载软件

(2) 软件下载完成后，会提示是否运行，如图 4-16 所示。下载之后可以直接使用，不需要安装的过程。



图 4-16 运行下载的软件

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 软件分类

(1) 云端软件平台，提供了大量的软件。在“推荐”中，有“联络聊天”、“音乐影视”、“网络应用”等多个分类。如果不熟悉某个软件，可以单击软件的名称，会显示软件的详细信息，如图 4-17 和图 4-18 所示。

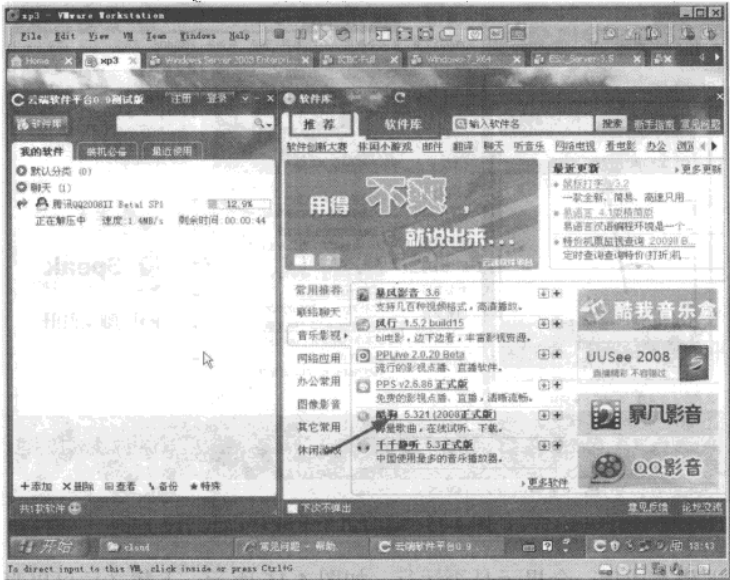


图 4-17 单击软件名称



图 4-18 显示软件的详细信息

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管员业余管理经验 4

(2) 在“软件库”中有更加详细的分类，用户可以查找自己所需要的软件，如图 4-19 所示。如果关闭了右侧的“软件库”，可以单击左侧的“软件库”按钮，重新打开软件分类列表。

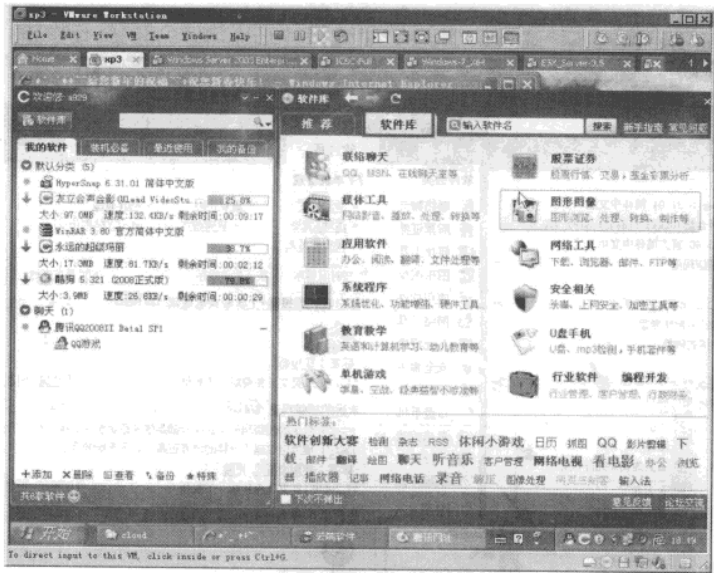


图 4-19 软件库

4. 软件运行与初始化

(1) 下面是运行超级玛丽的小游戏，如图 4-20 所示。

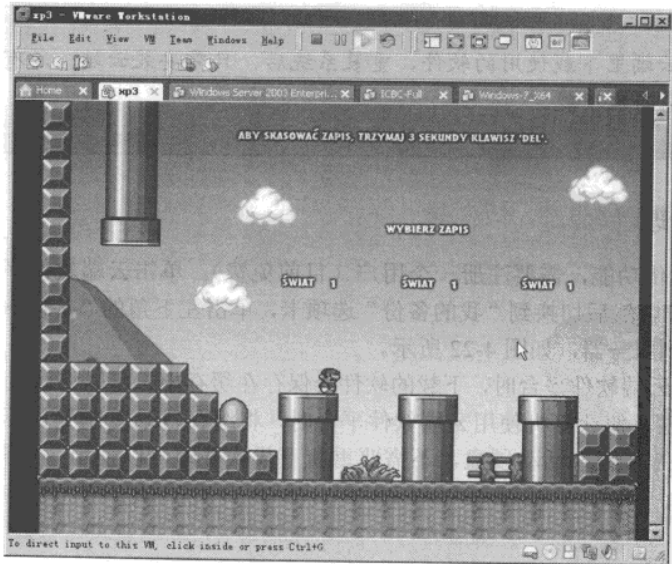


图 4-20 玛丽游戏

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

(2) 使用云端软件平台，如果某个软件配置错误，可以将软件恢复到下载时的状态，如图 4-21 所示。



图 4-21 软件设置

说明 在云端里下载使用的软件，重装系统后，只需安装云端，所有软件立即恢复，无需再次下载。

5. 软件管理

(1) 使用上传功能，需要注册一个用户（目前免费）。单击云端软件平台的“注册”按钮，注册一个用户，然后切换到“我的备份”选项卡，单击左下角的“备份→上传软件列表”，将软件列表上传到服务器，如图 4-22 所示。

(2) 在使用云端软件平台时，下载的软件会保存在缓存中，可以将此文件夹复制到 U 盘或移动硬盘，当在其他计算机使用云端软件平台时，将缓存目录复制到目标计算机，或者直接指定缓存目录在 U 盘或活动硬盘，不需要重新下载软件即可以使用，如图 4-23 和图 4-24 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

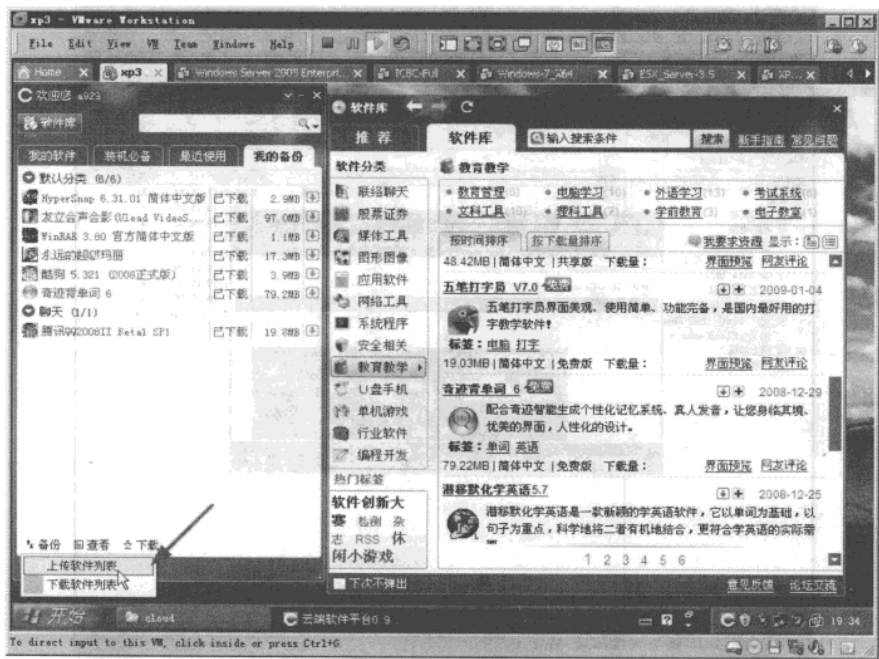


图 4-22 上传软件列表

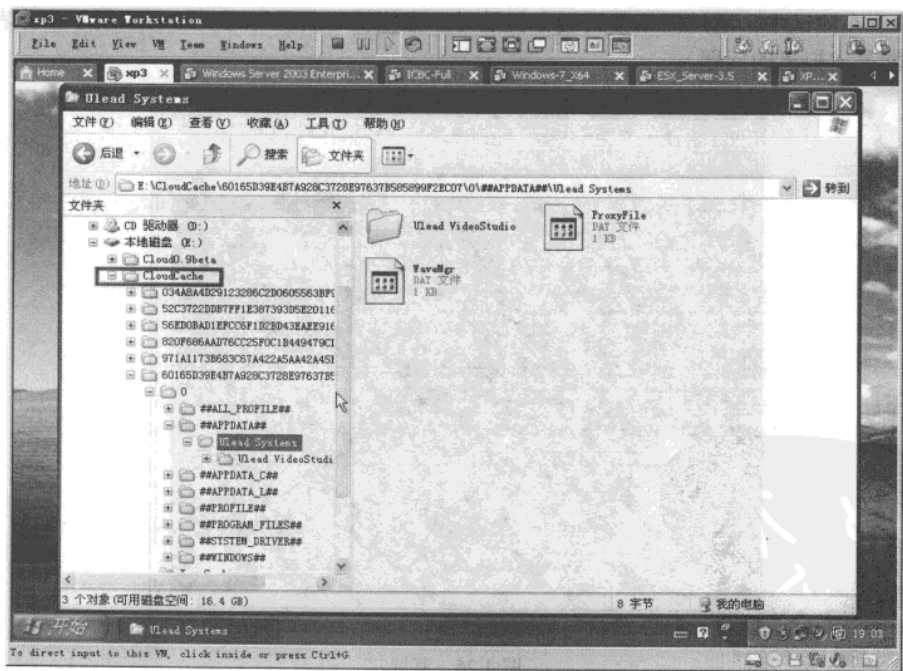


图 4-23 缓存目录

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

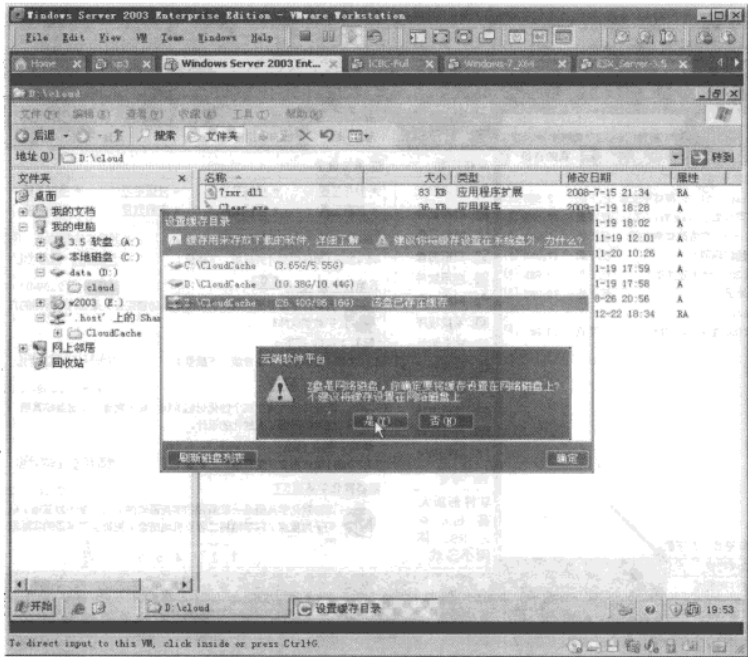


图 4-24 选择缓存目录

(3) 在测试中，通过网络使用缓存目录时，虚拟机“蓝屏”，如图 4-25 所示（作者认为这个可能是虚拟机的问题）。

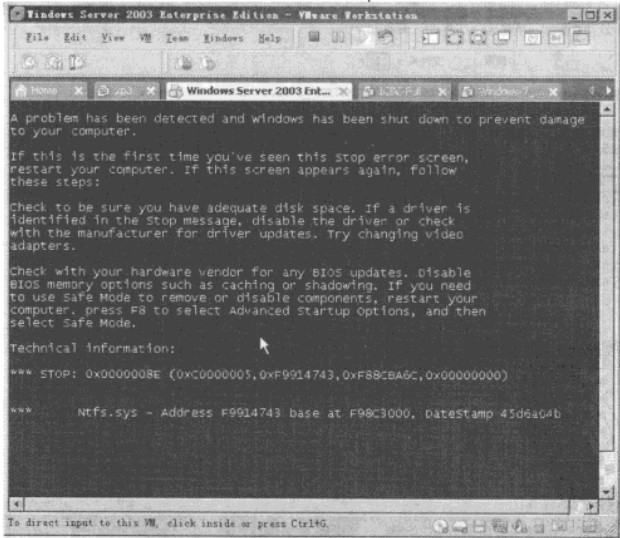


图 4-25 蓝屏

(4) 将缓存复制到虚拟机中，并修改 config.ini 配置文件，将缓存目录 Z 修改为 D，然后

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

就可以使用了，如图 4-26 和图 4-27 所示。

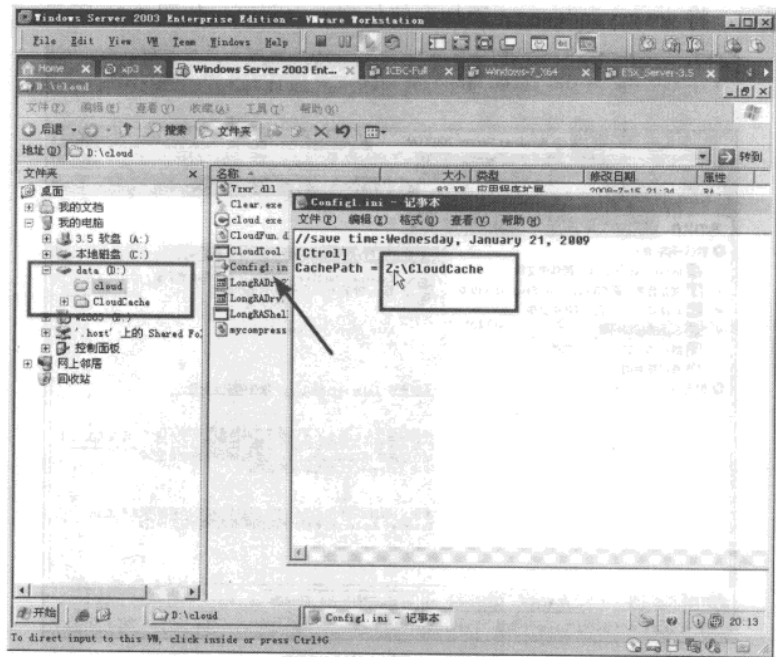


图 4-26 修改配置文件

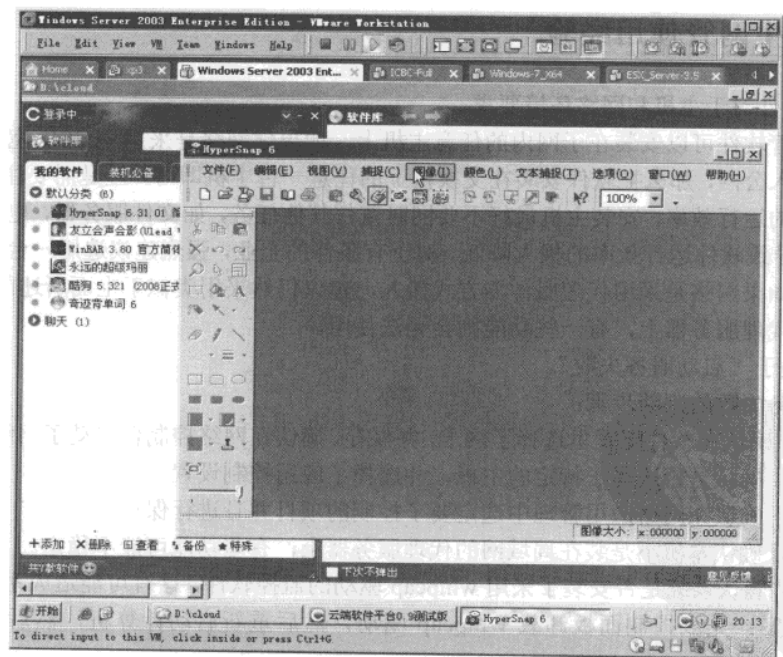


图 4-27 使用 HyperSnap

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

(5) 在 Windows Server 2003 上，如果启用了“使用增强的 IE 配置”，则在浏览软件库中，会弹出下表提示，将 **www.yunduan.cn** 添加到信任列表中即可，如图 4-28 所示。

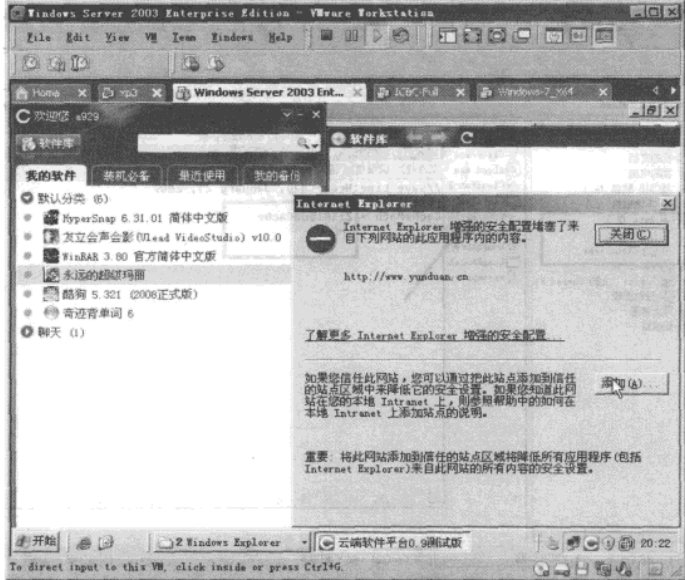


图 4-28 添加信任列表

4.2.2 聚生网管使用经验

(1) 软件对于主机和网络环境要求。

聚生网管软件可以安装在子网内的任意主机上，如果你网络是采用 ADSL 宽带路由器或者路由器接入公网，那么把软件安装在交换机上的任意一台主机即可，但是需要注意的是，为了保证软件的运行效率，安装主机最好不要同时兼任其他任务，如文件服务器，电影服务器之类，这样会导致软件运行效率的极大降低。对于有条件的企业，强烈建议选用一台专门主机作为控制机。如果网络是采用代理服务器方式接入，建议仍然采用类似于上面所述的安装方式，如果安装在代理服务器上，有一些功能则会无法使用。

(2) 关于“启动服务失败”。

启动服务失败的判断步骤：

- 第 1 步，确认在软件配置里选择了网卡，并保存。确认在网络控制台启动了网络控制服务。
- 第 2 步，确认是否选择了特定的主机，并选择了应用控制设置。
- 第 3 步，确认在网络应用管理中选定要了控制的项目并且进行保存。
- 第 4 步，确认本机不是装在局域网的代理服务器上，有些功能可能不稳定。
- 第 5 步，确认系统是否安装了采用 winpcap 驱动的监控软件，这有可能造成系统的无法运行。解决方案：先到控制面板卸载 winpcap 驱动，然后重新启动计算机，然后重新安装本软件。
- 第 6 步，确认局域网有没有进行 IP-MAC 绑定，如果已经进行了绑定那么运行本软件就会

导致局域网被控主机掉线。

第7步，确认计算机是否安装了其他类似的监控软件，如果有，请卸载后重新测试。

第8步，重新启动一下系统，因为有时候是你的系统环境有问题。

(3) 提示了系统控制 x.x.x.xP2P 下载信息，对方还能下载的问题。

因为 P2P 下载的特点就是不断的去连接新的 IP 地址，所以软件提示的信息表示正在拦截该主机连接更多的 IP，而已经建立的连接聚生网管是无法区分的，所以就会造成还有下载速度。解决方法：让聚生网管软件处于一直运行状态，这样新的 P2P 下载就会受到控制；或者限制发现 P2P 下载时的上行和下行速度，这样 BT 下载就会受到有效的抑制。

(4) 网络带宽查看里面显示的主机实时流量和在主机上查看的流量有差异。

因为聚生网管对网络主机的公网下行带宽是根据报文数采用一定算法进行估算而来，而不是根据字节计算，所以就有可能出现一定偏差，但是仍然可以在很大程度上准确反映出当前公网带宽占用情况。

(5) 对局域网的主机进行了限制后，导致主机不能上网的情况。

请查看是否在代理服务器上或者路由器中启用了 IP-MAC 绑定，如果启用，请取消绑定设置；可以使用聚生网管提供的 IP-MAC 绑定功能来实现绑定；因为聚生网管采用了虚拟路由技术，在被控制主机发出数据报文后，经过控制主机虚拟路由后，报文的源 MAC 地址会发生变化，而如果在代理服务器上或者路由器上启用了 IP-MAC 绑定，那么这种源 MAC 地址已经发生变化的报文就会被代理服务器或者路由器丢弃，从而造成被控制主机无法上网。另外，在软件运行的时候不能直接断电关机，或者按下 RESET 键直接重启计算机，否则可能造成局域网被控制主机暂时掉线。解决方法：正常退出软件或者正常关机，又或者在重启计算机后，重新启动软件控制，网络即可恢复正常。

(6) 主机名显示：“——”的问题。

这种情况下，一般是装有软件的主机没有安装 netbios 协议，系统不让查看计算机名。方法：右键单击“网上邻居”→属性”→“本地连接”→“属性”→“安装”→“协议”→“添加”→“NWLINK NETBIOS”。然后单击“确定”按钮，退出即可；如果仍有个别主机名无法显示，一般情况下就是对方主机开了防火墙，禁止了本地主机的查询，可以将其关闭即可。无论防火墙开启与关闭，均不影响程序的监控。

(7) 所有的控制都不能实现的问题。

确认在“网络控制台”中启动了“网络控制服务”；确认你在“网络应用管理”中设定了相关的限制项目，并且进行了保存；确认你在“网络主机扫描”中选定了某个主机或者全部主机。你也可以从本网站下载最新的聚生网管版本测试。

(8) 局域网 IP 冲突，由此导致不能上网。

如果启动网络控制后，有的主机总是出现 IP 地址冲突框，那么请查看是否已经启用了“网络安全管理”模块下面的“IP-MAC 绑定”，并且选定了下面的“发现非法 IP-MAC 绑定时，断开改主机公网连接”和“发现非法 IP-MAC 绑定时，发 IP 冲突给该主机”。如果选定，请取消。如果确认本局域网没有被其他软件实施 IP-MAC 绑定，那么就可以启用本系统的 IP-MAC 绑定，并且获取 IP-MAC 列表。然后选择下面的两项，这样就实施了本软件的 IP-MAC 绑定，保存退出。

4.2.3 制作 Windows Server 2008 中文版的经验

微软发布系统都是先发布英文版，过上一段时间后才会发布中文版。那么在这段时间里，网管员想先尝试一下新操作系统的优势，但很多时候却因为不习惯用英文版的系统而退缩了。作为网管为何不尝试一下自己制作中文版的操作系统呢。其实使用 Microsoft 提供的 AIK 工具包，就可以自己制作中文的 Windows Server 2008。本节就以 Windows Service 2008 为例介绍一下自己定制中文版操作系统的方法。

第 1 步，准备 Windows Server 2008 32 位英文版、32 位简体中文语言包，AIK 工具。下载地址：<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08> 下载“Automated Installation Kit (AIK) for Windows Vista SP1 还有“Windows Server 2008—简体中文”工具。下载地址：<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=e9f6f200-cfaf-4516-8e96-e4d4750397ff>

在下载的过程中，使用虚拟光驱加载 Windows Server 2008 英文版，并且找一个空间比较大的分区，将 Windows Server 2008 安装程序复制到一个文件夹中，本例为 E:\win2008-aik，另外再创建一个文件夹，本例为 e:\w2008cn，保证所在分区有至少 6 GB 空间。

第 2 步，下载之后，安装 AIK 工具。在安装之前，先安装“MSXML 6.0”与“Microsoft .Net Framework”程序，如图 4-29 所示。

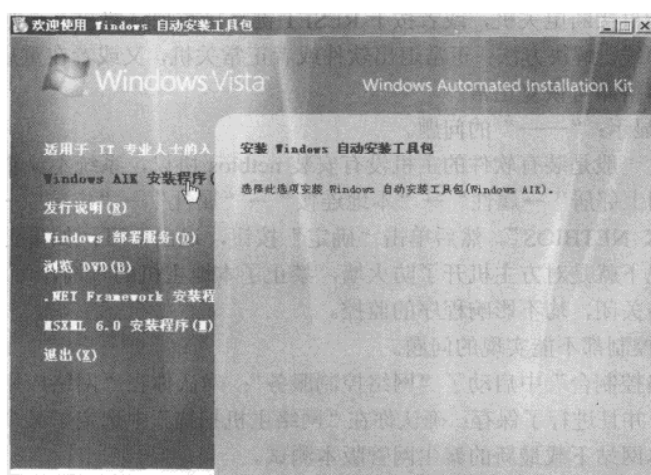


图 4-29 安装 Windows AIK

第 3 步，在“Microsoft Windows AIK”程序组中运行“Windows 系统映像管理器”，在“Windows 映像”中用鼠标右击“选择 Windows 映像或编录文件”选项，在弹出的快捷菜单中选择“选择 Windows 映像”命令，如图 4-30 所示。选择 Windows Server 2008 安装程序中的“install.wim”文件（在 e:\w2008-aik\sources 目录中），在弹出的“选择映像”对话框中选择一个，例如“Windows Longhorn SERVER ENTERPRISE”，表示选择企业版。

第 4 步，右击“应答文件”，在弹出的快捷菜单中选择“新建应答文件”命令，在左侧“Windows 映像”下面展开“Packages→LanguagePack”选项，在弹出的快捷菜单中右击选中

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

两个英文语言包，选择“添加到应答文件”命令，如图 4-31 所示。

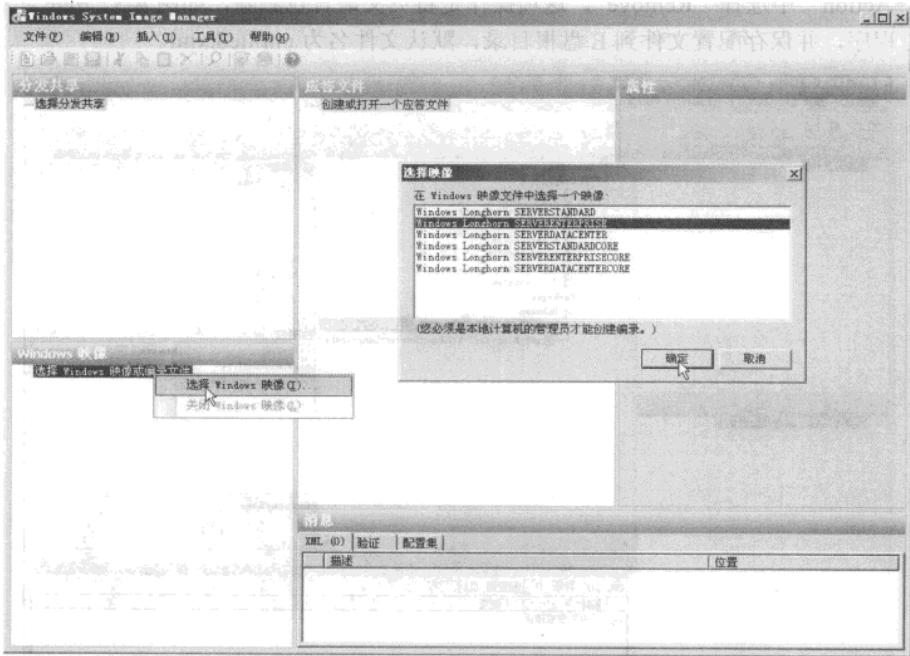


图 4-30 选择要制作的影像文件

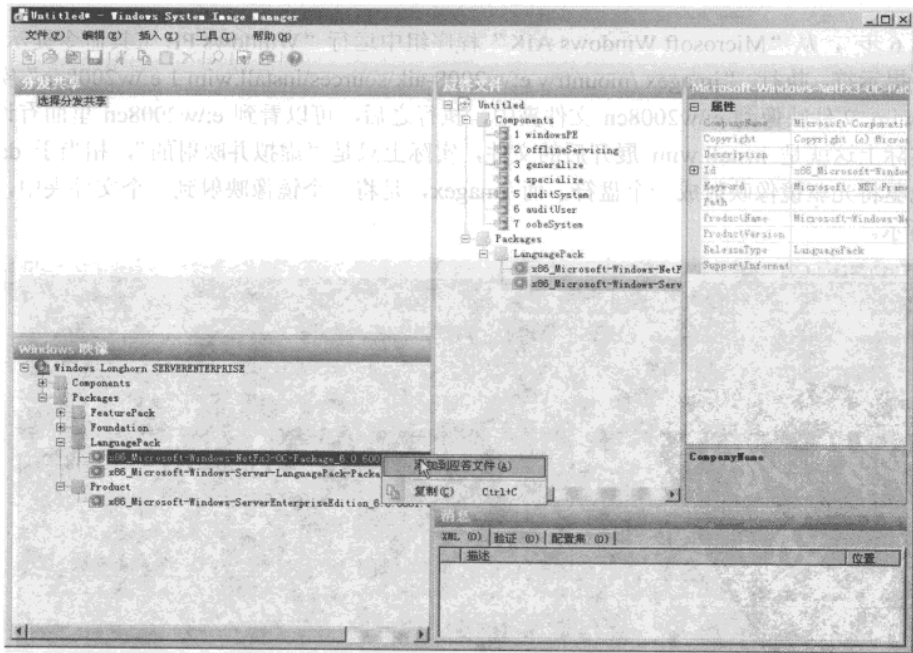


图 4-31 选择语言包

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 5 步，在图 4-31 所示中分别选中每一个语言包（x86_Microsoft-Windows...等），在右侧“设置→Action”中选择“Remove”，这项操作是将英文语言包删除，如图 4-32 所示。然后关闭 AIK 程序，并保存配置文件到 E 盘根目录，默认文件名为 untitled.xml。

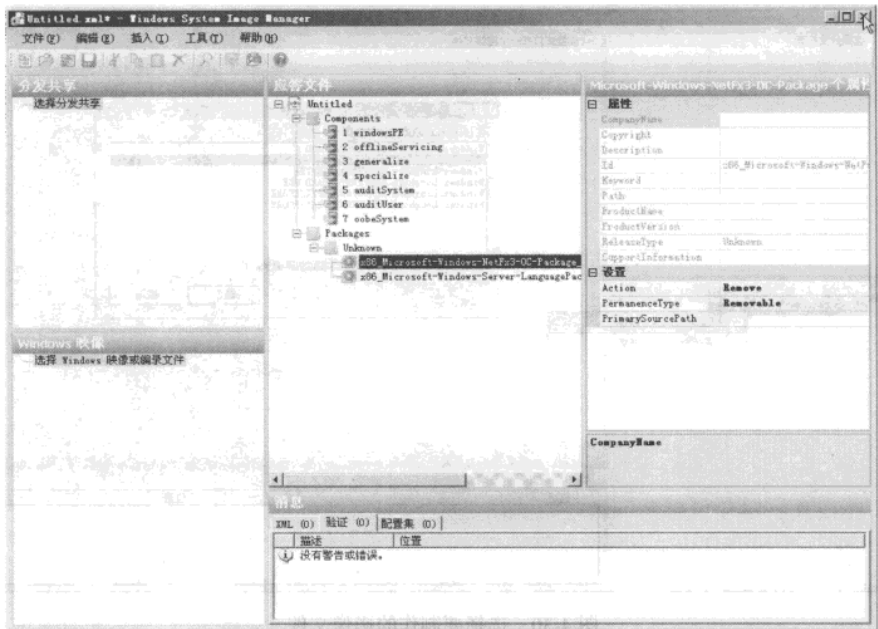


图 4-32 移除英文语言包

第 6 步，从“Microsoft Windows AIK”程序组中运行“Windows PE 工具命令提示”，进入命令提示符，执行“imagex /mountw e:\w2008cn\sources\install.wim 1 e:\w2008cn”实现将 install.wim 文件映像到 e:\w2008cn 文件夹中，执行之后，可以看到 e:\w2008cn 里面有许多文件，实际上这就是 install.wim 展开后的文件，实际上只是“虚拟并映射的”，相当于 daemon 虚拟光驱将光驱镜像映射成一个盘符，而 imagex，是将一个镜像映射到一个文件夹中，如图 4-33 所示。

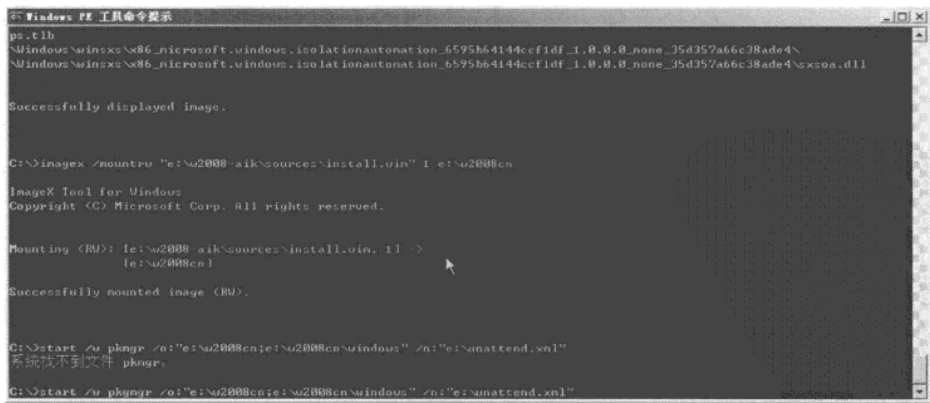


图 4-33 虚拟并映射影像文件

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 7 步，执行 “start /w pkgmgr /o:"e:\w2008cn;e:\w2008cn\windows" /n:"e:\untitled.xml” 命令，如果提示找不到 pkgmgr 文件，如图 4-34 所示。则可以在命令提示符下执行 dir c:\pkgmgr.exe /s 搜索到并复制到当前目录即可。

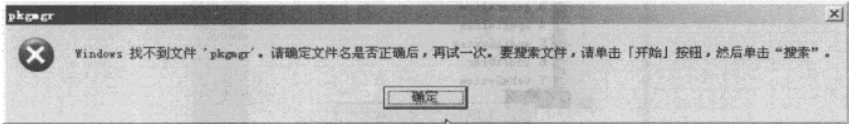


图 4-34 错误提示

第 8 步，执行 “peimg /list e:\w2008cn\windows” 命令，显示 e:\w2008cn 目录中是否包括英文的语言包，如果仍然显示 EN-US 语言包，可能是在执行 Start 命令时，配置文件名不对，检查或重执行命令 “start /w pkgmgr /o:"e:\w2008cn;e:\w2008cn\windows" /n:"e:\untitled.xml” 直至显示 “8 个程序包” 为止，如图 4-35 所示。

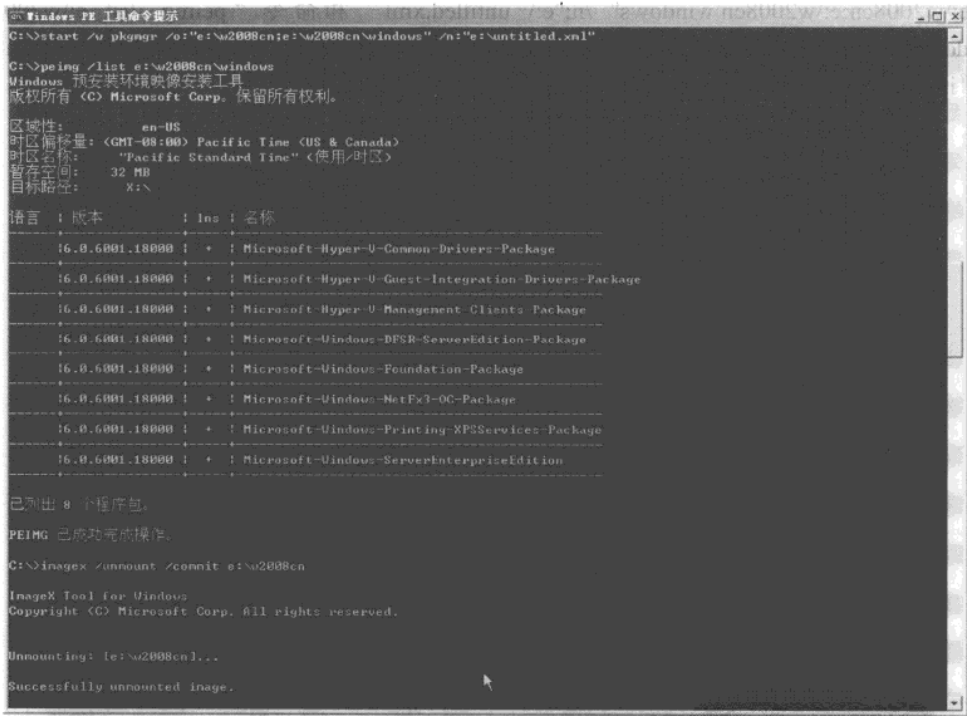


图 4-35 查看英文语言包是否移除

第 9 步，执行 “imagex /unmount /commit e:\w2008cn” 命令，实现更新 install.wim 映像的功能。

第 10 步，安装中文语言包：运行 AIK 映像管理器，通过管理器打开刚才的 install.wim，在应答文件栏右击 “Packages→插入数据包”，在弹出的快捷菜单中选择 “Windows Server 2008 中文语言包” 选项，然后保存应答文件并退出 AIK，如图 4-36 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

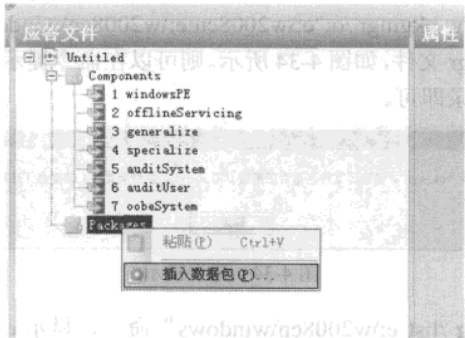


图 4-36 添加中文语言包

第 11 步，将语言包添加到镜像中，切换到“Windows PE 工具命令提示”窗口，继续执行下面的命令：“imagex /mounttrw e:\w2008-aik\sources\install.wim 1 e:\w2008cn”、“start /w pkgmgr /o:"e:\w2008cn;e:\w2008cn\windows" /n:"e:\untitled.xml" 和命令 “peimg /list e:\w2008cn\windows”，修改 lang.ini 文件“intlcfg-genlangini-dist:e:\w2008-aik-image:e:\w2008cn -all:zh-cn”和 “imagex /unmount /commit e:\w2008cn”，如图 4-37 所示。



图 4-37 修改 lang.ini 文件

第 12 步，解压缩中文语言包 lp.cab 到一个目录中，复制\zh-cn\setup\sources\目录下的 zh-cn 文件夹到 e:\w2008-aik\vista\sources\根目录下，把\zh-cn\sources\license\目录下的 zh-cn 文件夹复制到 e:\w2008-aik\sources\license\目录下。

第 13 步，更新 BOOT.wim 文件：执行“`imagex /mounttrw e:\w2008-aik\sources\boot.wim 2 e:\w2008cn`”命令，然后把 `e:\w2008-aik\sources\` 下的除了两个 WIM 文件的所有文件都复制到 `e:\w2008cn\sources` 文件夹内，替换里面所有文件。然后执行“`imagex /unmount /commit e:\w2008cn`”命令。

第 14 步，执行“`imagex /mounttrw e:\w2008-aik\sources\install.wim 1 e:\w2008cn`”命令，然后打开 `e:\w2008cn\windows\system32\oobe\zh-cn` 文件夹，把里面的 5 个 `rtf` 文件复制到 `f:\w2008-aik\sources\zh-cn` 文件夹里。再执行“`imagex /unmount /commit e:\w2008cn`”命令。

第 15 步，最后执行“`oscdimg -n -be:\w2008-aik\boot\etfsboot.com e:\w2008-aik e:\w2008entcn2.iso -o -m`”命令，实现打包成 ISO 镜像的功能。

第 16 步，在 VMware 虚拟机中测试，在安装的前几步是英文，如图 4-38 所示。在重启一次之后，再进入安装界面时将会显示中文，如图 4-39 所示。

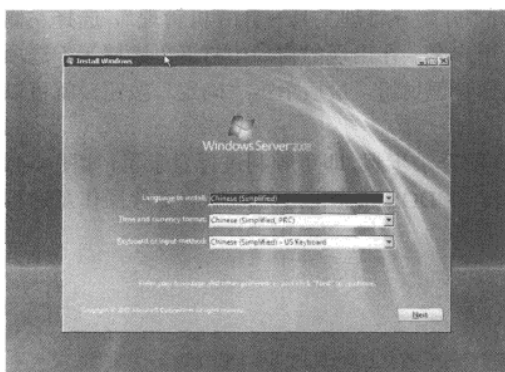


图 4-38 英文安装界面

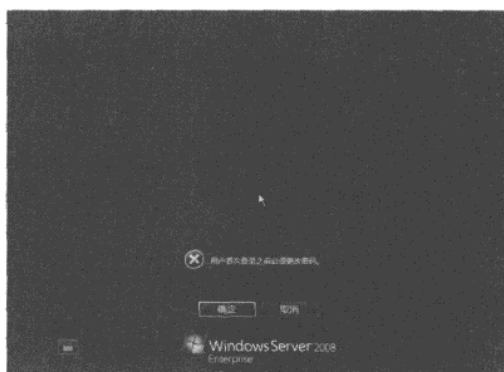


图 4-39 中文界面

4.2.4 利用 Win XP 自带工具实现远程管理

在 Win XP/2003 等操作系统中可以使用“远程协助”和“远程桌面”这两种功能实现远程控制。另外，一些第三方软件也能进行远程控制，但这些图形化界面对网络带宽很小的用户而言，就意味着要花费更多的时间，以及增加网络数据传输中断的几率。

其实，若是进行一些简单的远程管理工作，利用 Win XP 操作系统自带的 Telnet 是一个不错的选择。在此我们就以 Win XP 操作系统作为客户端，Win 2003 作为服务端为例进行 Telnet。

启动 Telnet 服务正常情况下在 Win 2003 操作系统中，我们可进入到系统命令提示符环境，输入“`net start Telnet`”后按 Enter 键便可开启 Telnet 服务。但若是出现“无法启动服务”这样的提示，那是因为系统中的 Telnet 服务并没有开启。

依次打开“开始→管理工具→服务”选项，在打开的“服务”窗口右侧服务列表中双击其中的“Telnet”，在打开的对话框中可发现“启动类型”为“已禁用”，而“服务状态”处于“已停止”状态。我们可将“启动类型”设为“自动”，单击“启动”按钮，就可以启动 Telnet 服务，如图 4-40 所示。

在 Win XP 客户端中，可进入命令提示符窗口，在提示符后按如下要求输入：Telnet 主机名（或 IP 地址）端口号，比如“`Telnet 171.171.151.117`”。

网管天下 网管经验谈

提示 在此可能有些读者朋友会发现作者在例子中并没有输入端口号，这是因为在服务器端，默认的 Telnet 服务端口号是 23，如果该服务的端口号有所变动，那么就要在命令中添加相应的端口号。输入完毕后，按 Enter 键便可进行登录。

在进行登录时，会出现一个“你将要把你的密码信息送到 Internet 区内的一台远程计算机上，这可能不安全。你还要发送吗？”这样的提示，为了安全起见，我们可输入“n”，这样便可有效地保证密码安全。

在随后出现一个登录提示，可分别在 login 和 passWord 后输入对方计算机赋予的用户名及密码，然后按 Enter 键，却出现了“用户不是 Telnet 客户端组成员，跟主机连接中断”这样的提示，出现这种情况的原因在于登录用户没有取得相应的管理权限。

我们可以返回到 Win 2003 服务端，依次打开“开始→管理工具→计算机管理”，选择左侧列表中的“用户”选项，双击右侧窗口中的登录用户名，在出现的窗口中打开“隶属于”选项卡，单击“添加”按钮，在“选择组”窗口中选择管理员组，最后单击“确定”按钮，就可以使用该用户具备管理权限。

最后返回到 Win XP 客户端，按照上面 Telnet 的登录步骤，即可顺利进行登录了，如图 4-41 所示。现在我们已经可以对服务端进行远程控制，在 DOS 状态下进行简单的文件操作及远程管理工作了。

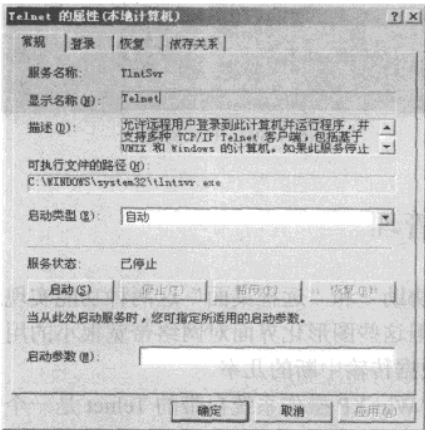


图 4-40 进行 Telnet 连接

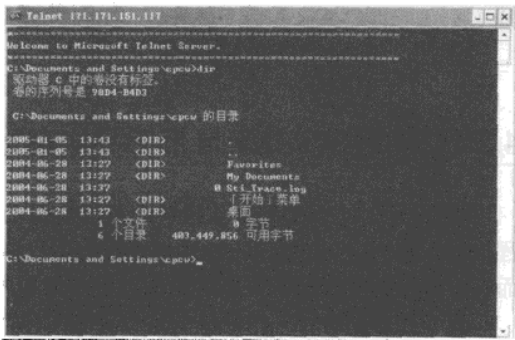


图 4-41 远程登录管理

第 5 章 虚拟化应用方面

现在计算机硬件的发展速度越来越快，成本越来越低，而与之伴随的计算机应用却没有跟上，造成服务器的资源浪费越来越严重，而要解决这个问题一个主要出路，就需要采用虚拟化来解决。虚拟化产品很多，对于网络管理员来说也都很有用。本章先具体的介绍现有的虚拟化产品及一些相关应用案例，接下来介绍 3 个使用 VM 虚拟机的小经验，最后是介绍一些用 VM 虚拟机做实验的经验。

5.1 虚拟化产品及应用举例

虚拟化产品有很多如 VMware 公司和 Microsoft 公司都有一系列的虚拟化产品。本节先对现有的虚拟化产品一一做了简单介绍，并对虚拟化产品的应用做了些介绍。接下来分别通过一个实例和一种经验来对 VM 虚拟机的应用做以下介绍。

5.1.1 虚拟化应用总结

1. 虚拟化介绍

在虚拟化方面，当今市场上最流行的主要有 VMware 公司的 VMware Server、VMware Workstation、VMware ACE、VMware ESX Server 系列产品，与 Microsoft 公司的 Microsoft Virtual PC 2007、Virtual Server 2005、Windows Server 2008 集成的 Hyper-V 系列产品。其中 VMware 产品线最全、提供虚拟化产品的时间最长、市场占有率最高。除了这些虚拟化产品之外，每个公司还有与之相对应的管理工具，例如 VMware 公司的 Virtual Center 系列、Microsoft 公司的 system center 系列。本节就给大家具体介绍一下以上这些产品。

(1) VMware Workstation。

VMware Workstation 是 VMware 公司的第一个虚拟化产品，它是一个提供“虚拟机”的产品，可以在一台正在运行 Windows 或 Linux 的主机操作系统上，使用 VMware Workstation 这个产品，可以为用户同时提供多台“虚拟计算机”，这些“虚拟机”像真实的计算机一样，可以安装不同类型（例如 Windows、Linux、Netware 等）、不同版本（例如 Windows 98、Windows Vista、Red Hat Linux 8.0 等）的操作系统，并且在操作系统上安装各种应用软件。

VMware Workstation 提供的多台虚拟机是互不干扰的，每台虚拟机都可以单独启动与运行。它主要面向 IT 企业的管理员、虚拟机爱好者、程序开发人员、网络管理员等专业用户，用于产品的测试、实验等。

VMware Workstation，是目前所有虚拟机类产品（包括 VMware 与 Microsoft 系列）功能最全、使用最方便、支持的操作系统最多的产品。如图 5-1 所示为在 VMware Workstation 中运行 Windows 2008 操作系统。

网管天下 网管经验谈

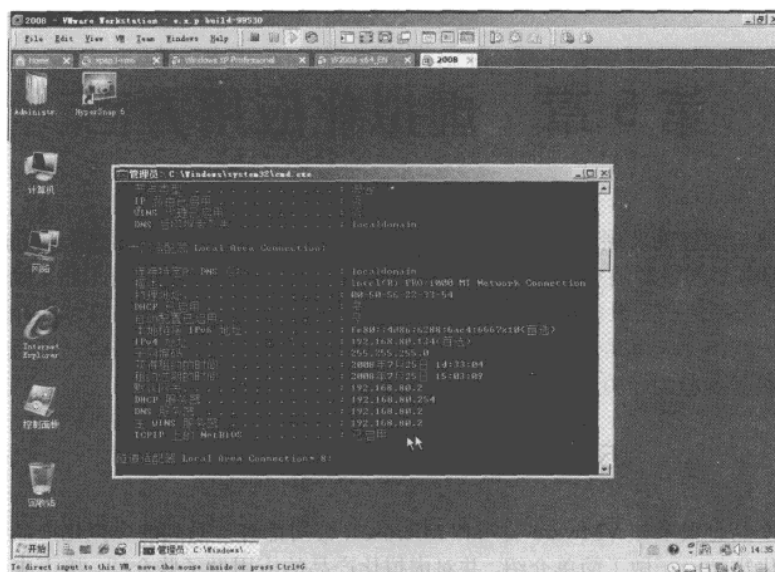


图 5-1 VMware Workstation 运行界面（虚拟机中安装的是 Windows Server 2008）

（2）VMware Server。

VMware Server 的前身是 VMware GSX Server，它运行于 Windows 或 Linux 主机操作系统，主要用于中小企业的“服务器”虚拟化。VMware Server 是一款免费产品。

VMware Server 的虚拟机可以在系统启动时“自己”启动，不需要用户再进入 VMware Server 运行。可以在一台高配置的服务器中，通过 VMware Server 及其支持的虚拟机，使其同时作为多台服务器使用。

VMware Server 的特点如下：

- ① VMware Server 是一款“商用”产品，它可以在一台物理主机上最多同时运行 64 台虚拟机。
- ② VMware Server 不需要登录进入系统，而是在主机启动之后即可以自动运行 VMware Server 中指定的虚拟机。
- ③ VMware Server 提供远程（可以使用 IE、也可以使用其专用客户端）管理工具，也可以使用 VMware VirtualCenter（VMware 虚拟中心）进行远程管理。
- ④ VMware Server 提供“一次快照”的保存与还原能力，并且可以“锁定”快照。

VMware Server 全面支持 32 位主机系统和 64 位主机系统（AMD 64 和 Intel 64 位处理器）。VMware Server 可以运行在 Windows 2000 及其以上的 Windows 平台和多种 Linux 平台上。VMware Server 支持 DOS、Windows、Linux 等多种虚拟机。

（3）VMware ACE。

VMware ACE 是用于企业终端的“虚拟化”解决方案，VMware ACE 是为那些想迅速提高企业的 PC 环境的安全性和标准化的 IT 桌面管理者准备的企业解决方案。VMware ACE 易于安装，提高了安全性和可管理性，并降低了公司 PC 的成本。VMware ACE 使 IT 桌面管理者能够对虚拟机应用企业级 IT 策略，这包括操作系统、企业应用程序和为特定的计算环境创

建的独立 PC 环境使用的数据。VMware 特定的计算环境是一个私有策略，提供对企业数据的保护和对企业允许的安全访问。

VMware ACE 在企业环境中的作用：

- 为无托管远程 PC 机提供企业标准的 PC 环境。
- 为无托管 guest PC 机提供时间受限的、锁定的 PC 环境。
- 保护移动 PC 上敏感的企业信息和个人信息。
- 为任何企业 PC 机提供标准化的独立于硬件的 PC 环境。

图 5-2 所示为启用 ACE 功能的 VMware Workstation 的运行界面。

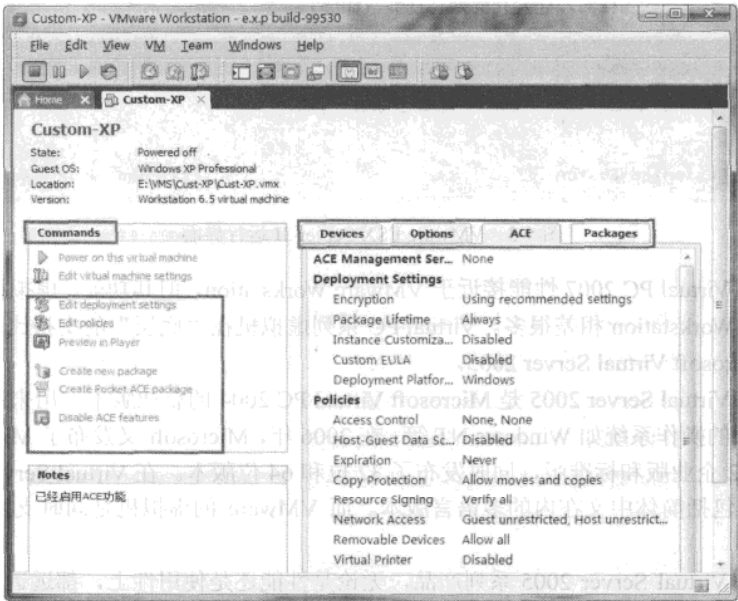


图 5-2 启用 ACE 功能的 VMware Workstation

(4) VMware ESX Server。

VMware ESX Server 是 VMware “企业级”的产品，它不需要底层操作系统的支持，可以直接运行在“裸机”上。

受到 Microsoft 推出 Hyper-V 产品的压力，在 2007 年 7 月底，VMware 宣布 VMware ESX 3I 免费。

VMware ESX 3i 可在单台服务器上为最占用资源的应用程序提供高性能的分区，同时允许你在几分钟内完成从启动到运行虚拟机的过程。它占用的空间只有 32 MB，从而在最大程度上减少了执行安全强化、用户访问控制以及备份过程所需的资源。VMware ESX 3I 采用与 VMware ESX 相同的构建技术，是市场领先的虚拟机管理程序，VMware 有 86% 的客户已在生产环境中部署了这一产品。如图 5-3 所示为 VMware ESX Server 3I 运行界面。

(5) Virtual PC 2007。

Microsoft Virtual PC 的前身是 Connectix 公司的 Virtual PC，它是一款与 VMware Workstation 相类似的虚拟机软件，它同样允许你在不改变现有硬盘分区的情况下，使用硬盘

网管天下 网管经验谈

空间安装多种操作系统。

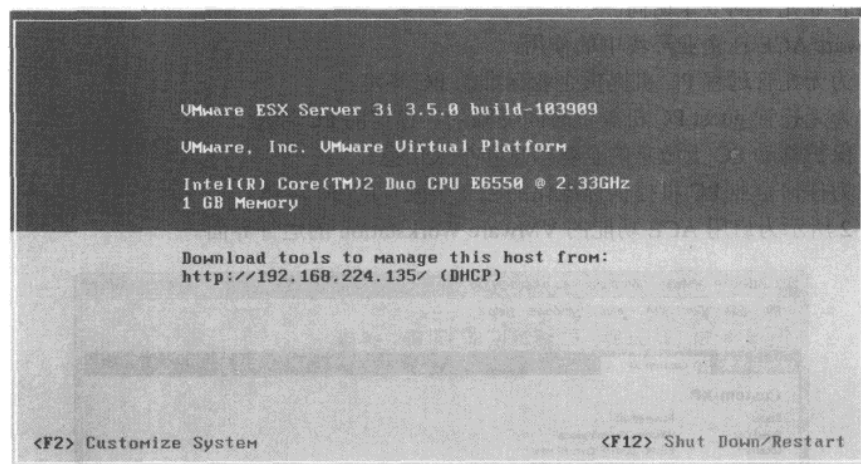


图 5-3 VMware ESX Server 3i 运行界面

Microsoft Virtual PC 2007 性能接近于 VMware Workstation，但其功能、虚拟机网络支持方面与 VMware Workstation 相差很多。Virtual PC 系列虚拟机在“底层”的支持比较好。

(6) Microsoft Virtual Server 2005。

Microsoft Virtual Server 2005 是 Microsoft Virtual PC 2004 的企业版本，用来迁移服务器和 Microsoft 旧版的操作系统如 Windows NT 等。在 2006 年，Microsoft 又发布了 Microsoft Virtual Server 2005 R2 企业版和标准版，同时发布了 32 位和 64 位版本。在 Virtual Server 2005 R2 版本中，发布了包括简体中文在内的多语言版本。而 VMware 的虚拟机是同时支持 32 位和 64 位系统的。

Microsoft Virtual Server 2005 系列产品，无论是性能还是使用性上，都远远低于 VMware Server 系列产品。

(7) Hyper-V。

Hyper-V 是 Windows Server 2008 X64（64 位）产品中集成的虚拟化产品。在 Windows Server 2008 发布时，其集成的 Hyper-V 是一个测试版本，而它的正式版本是在 2008 年 6 月份发布的。

Hyper-V 是 Microsoft 发布的挑战 VMware ESX Server 系列的产品，从产品线上来看，它对应于 VMware ESX Server。

VMware 作为业内“领头”的虚拟化软件提供厂商，从 1998 年起即开始提供虚拟化产品，其产品线全、产品稳定性高，在当前及未来的一段时间内仍然是市场的主宰。目前市场上应用的虚拟化产品有 80% 以上是 VMware 所提供的，所以本文将主要介绍 VMware 虚拟化产品在生产、生活中的应用，辅以介绍 Hyper-V 产品应用，这包括：迁移证券公司的 Netware 服务器解决方案，迁移（合并）政府部门 Windows 服务器解决方案、VMware ACE 应用专题及 Hyper-V 的使用。Hyper-V 的使用界面如图 5-4 所示。



图 5-4 在 Hyper-V 虚拟机中安装驱动程序

2. 迁移（合并）政府部门的 Windows 服务器解决方案

VMware Converter 3.0 是 VMware 提供的迁移工具，可以将运行 Windows 操作系统的物理主机直接“迁移”到 VMware 虚拟机中，本节以一个真实的案例为背景，介绍迁移 Windows 服务器到 VMware 虚拟机的方法、步骤，以及迁移过程中碰到的问题以及注意事项。

(1) 迁移 Windows 服务器的应用背景。

在政府、机关与事业单位中有许多办公网站，每个办公网站都放在一台单独的服务器中，这些服务器大多是 HP、IBM 等高档服务器，但这些服务器大多只配置了两块硬盘（做成 RAID1），这样造成了比较大的浪费，原因如下：

- ① 服务器利用率低：经过实际观测，大多数网站（或其他应用）只占用了 20 MB~3 GB 不等的空间，CPU 使用率大多在 2%~5%左右。
- ② 服务器磁盘性能比较低：大多数服务器都使用了 RAID1 磁盘阵列，效率低、浪费大、速度慢。在向 RAID1 的磁盘阵列中写入数据时，有效速度是原来单块硬盘的一半，读数据速度与原来单块硬盘相同。虽然服务器都配置了 320 MB/s 的 SCSI 接口与 RAID 卡，但由于单块硬盘的读写速度大约在 52 MB/s，所以，在实际使用中，写入速度只有 26 MB/s，读速度大约在 52 MB/s。现在的服务器，其 SCSI 卡与 RAID 卡都支持双通道 320 MB/s 的速度，如果配置 RAID1，远远达不到接口的速度。如果采用 RAID5 并配置多块硬盘，可以达到 640 MB/s 的理论速度。
- ③ 能耗大：所有的服务器 24 小时对外提供服务，以 10 台服务器机房耗电为例，假设每台服务器每小时耗电 650 W，以河北省（工业）用电每度 0.6527 元计算，每台服务器每年所需电费大约=650W/小时×24 小时/天×365 天/年×0.6527 元/（KW.H）÷1000=3 716 元，则 10 台服务器需要 37 160 元；如果再加上两台空调的电费（以每台空调 220 W 计算）=220 W/

网管天下 网管经验谈

小时 $\times 24$ 小时/天 $\times 365$ 天/年 $\times 0.6527$ 元/(KW.H) $\div 1000 \times 2 = 2\,516$ 元；在不计算照明等其他费用的情况下，这个机房年耗电需要 39676 元的电费。

从以上数字可以看出，每台服务器的浪费是比较惊人的，同时服务器的使用率、效率、速度也很低。如果使用虚拟化技术，将多台服务器迁移到 1 到 2 台虚拟机中，并且对服务器的硬盘进行合理的“合并”使用，将会提高现有网站访问速度的情况下节省能源消耗，同时可以减轻服务器的数量。下面，将通过一个具体的案例，介绍将多台物理服务器迁移到两台虚拟机中的方法与详细步骤。

A 市政务服务中心，有 7 台服务器，存在 11 个网站，其中有 3 台 IBM 3650，3 台 HP 3850，1 台 IBM x Series，保存的 11 个网站名称及 IP 地址如下：

A 市网上 Internet 审批系统，192.168.2.199

A 市项目建设管理系统，192.168.2.198

A 市企业基础信息系统，192.168.2.196

A 市车辆基础信息系统，192.168.2.199

A 市非税收入管理系统，192.168.2.99

A 市税源监控分析系统，192.168.2.99

A 市人事信息查询系统，192.168.2.197

A 市综合数据信息系统，192.168.2.196

A 市诚信数据查询系统，192.168.2.200

A 市地理信息查询系统，192.168.2.202

另外，A 市党政公务网，也保存在 192.168.2.199 的服务器上。

其中，各服务器的配置如下：

IBM 3650 是 2 GB 内存，两个 73 GB 的 SCSI 硬盘，做的 RAID1；HP 3850 是 4 GB 内存，两块 146 GB 的 SCSI 硬盘，做的 RAID1，而 IBM x Series 是一块硬盘，1 GB 内存，73 GB 硬盘。IBM 3650 与 HP 3850 都是两块千兆位（电接口）网卡，每台服务器最多可以插 6 块 SCSI 硬盘。

（2）合并与迁移服务器的指导思想。

针对本节中的案例，在与客户沟通后，定下如下的解决方案：

① 将原来所有运行在 HP 服务器上系统（操作系统、数据库与网站），整体迁移到其中的一台 IBM 服务器上；将原来所有运行在 IBM 服务器上的系统（包括 3 台 IBM 3650 与 1 台 IBM x Series）迁移到其中的一台 HP 3850 上。

② 将其中一台 IBM 服务器的内存升级到 8 GB，并重新购买 6 块 73 GB 的 SCSI 硬盘，组成 RAID 5 的磁盘阵列。

③ 将其中的一台 HP 3850 内存升级到 8 GB，并重新购买 6 块 146 GB 硬盘，组成 RAID 5 磁盘阵列。

④ 在迁移的过程中，为了保证数据不出问题，所有服务器上原来的硬盘都会贴上标签并予以保留，在完成迁移的一周后，在确认所有的迁移都完成，并且系统运行正常、数据无误后，节省下来的服务器再做他用。

在迁移的过程中，因为这 7 台服务器要迁移到其中的两台服务器中以“虚拟服务器”的形式运行。所以，在迁移的时候，是有一定技巧的，为了保证数据，一般情况下，要采用下列的方法：

① 将所有的服务器贴上标签，以示区分。例如，将 3 台 IBM 3650 贴上标签，分别用 3650-1、3650-2、3650-3 区分，将 3 台 HP 3850 用 3850-1、3850-2、3850-3 区分，将 IBM x Series 用 IBM-4 区分。

② 假设要将所有的 IBM 服务器迁移到 3850-2 服务器上，假设要将所有的 HP 服务器迁移到 3650-2 上。这时候，需要先迁移原 3850-2 或 3650-2 系统到虚拟机中，然后再在这两台服务器上扩充内存、拆下旧硬盘（贴标签）、添加新硬盘，迁移其他服务器到该服务器中。

在迁移的过程中，需要找一台服务器做“中转”，才能完成所有系统的迁移。下面给出迁移的方法，仅供参考：

① 检查各服务器使用的硬盘空间，以及可用的硬盘空间。在检查之后，可以将使用硬盘空间最小的一台服务器，迁移到可用硬盘空间最大的服务器中。例如，将 3650-2 迁移到 3850-3 中，有关迁移的步骤与方法将在下面介绍。

② 将 3650-2 成功迁移到 3850-3 后，关闭 3650-2，拆下 3650-2 的两块 73 GB 硬盘，并贴上标签，保存在安全的位置。然后将 3650-2 的内存，扩充到 8 GB，并插上新购买的 6 块 73 GB 硬盘。在默认情况下，IBM 3650 不支持 RAID5，需要为 IBM 3650 购买 RAID 卡，该 RAID 卡是一个类似于外观、大小类似于内存的插件，要插在服务器的扩展槽上，并需要拆下原来的 RAID 卡（原来的 RAID 卡只支持 RAID0 与 RAID1）。

③ 在完成扩充内存、装上新硬盘后，重新开机，进入 RAID 卡控制程序，将这 6 块新 73 GB 硬盘，使用 RAID 5 方式，创建两个逻辑磁盘，其中第 1 个逻辑磁盘 40 GB 大小，剩余的空间作为第 2 个逻辑磁盘（ $73 \text{ GB} \times 5 - 40 \text{ GB} \approx 320 \text{ GB}$ ）。

④ 划分逻辑磁盘后，安装 64 位的 Windows Server 2003 企业版，在安装的过程中，将操作系统安装在第 1 个逻辑磁盘上，并且在第 1 个逻辑磁盘上只创建 1 个分区。安装完成后，将第 2 个逻辑磁盘创建 1 个分区，该分区卷标为 VMS。同时，要为该主机设置 IP 地址，IP 地址与原来的主机在同一个网段，例如，可以设置 192.168.2.50 等，要使用一个“空闲”的 IP 地址。

⑤ 在该服务器上安装 VMware Server 1.05。然后，将原 3650-2 的虚拟机镜像（在第（1）步中迁移到 3850-3）从 3850-3 复制到该服务器的 D 盘（卷标为 VMS），并从 3850-3 上删除该镜像。

⑥ 将 HP 3850-1、3850-2、3850-3 迁移到 3650-2。

⑦ 迁移之后，关闭 HP 3850-1、3850-2、3850-3，并拆下 3850-2 的硬盘，贴上标签，保存在安全位置。然后扩充内存到 8 GB，添加新购买的 6 块 146 GB 硬盘，组建 RAID 5，组建的过程中，也是创建两个逻辑磁盘，第 1 个逻辑磁盘为 50 GB，第 2 个逻辑磁盘大约为 $146 \times 5 - 50 \text{ GB} \approx 680 \text{ GB}$ 。

⑧ 在 HP 3850-2 的第 1 个逻辑磁盘上安装 Windows Server 2003 的 64 位操作系统，将第 2 个逻辑磁盘划分为一个分区。然后安装 VMware Server 1.05。

⑨ 将其他 IBM 服务器（排除 3650-2）迁移到 HP 3850-2 服务器中，然后从 3650-2 中将原 3650-2 虚拟机镜像复制到 HP 3850-2。

⑩ 分别在 IBM 3650-2 与 HP 3850-2 上，加载迁移后的虚拟机，完成迁移。

（3）使用 VMware Converter 迁移 Windows 服务器。

VMware Converter 是 VMware 推出的一款可以将物理机转化为虚拟机的软件，它可以快速将基于 Microsoft Windows 的物理机和第三方映像格式转换为 VMware 虚拟机。它还可以在两个 VMware 平台之间转换虚拟机。使用 VMware Converter，可以自动化和简化物理机到

虚拟机以及虚拟机格式之间的转换过程。

3. 迁移前的注意问题

使用 VMware Converter 迁移服务器时，虽然可以在不中断物理服务器运行的情况下迁移，并且可以对物理服务器不做任何更改就可以完成迁移，但在真正的迁移中，遵循下列原则，可以提高迁移的成功性，并且可以加快迁移的速度。

- (1) 在迁移之前，断开网络，最好是使用 RJ45 的直通线，将“源”服务器与“目的”服务器连接在一起，这样在迁移的过程中，将会以最大的网络速度进行。
- (2) 停止“源”服务器的 SQL Server 服务、退出杀毒软件的运行，关闭“源”与“目的”服务器的防火墙。
- (3) 使用 chkdsk 命令，检查“源”服务器磁盘是否有错误，并进行修复。
- (4) 如果“源”服务器上有一些与服务无关的数据，例如一些安装程序、光盘镜像等，可以将这些数据“移动”到“目的”服务器的主机上，以后再使用时，直接通过网络共享文件夹使用，这样可以减少迁移的数据量。

4. VMware Converter 使用

在本节中，将把 IP 地址为 192.168.2.199 的物理主机，通过网络、迁移到 IP 地址为 192.168.2.196 的服务器上，并且直接保存成虚拟机的格式。使用 VMware Converter 可以很方便的完成从物理机到虚拟机的转换，在转换的过程中，还可以直接通过网络，将转换后的虚拟机保存在远程服务器上。

- 第 1 步，在 IP 地址为 192.168.2.199 的物理主机上，安装 VMware Converter 3.03。
- 第 2 步，运行 VMware Converter 标准版，在使用的时候，单击“Continue in Starter Mode”按钮，进入 VMware Converter 主界面。
- 第 3 步，在 VMware Converter 主界面中，单击“Convert Machine”按钮。
- 第 4 步，在“Select the type of source you want to use”下拉列表框中选择“Physical Computer”选项，然后单击“下一步”按钮，如图 5-5 所示。

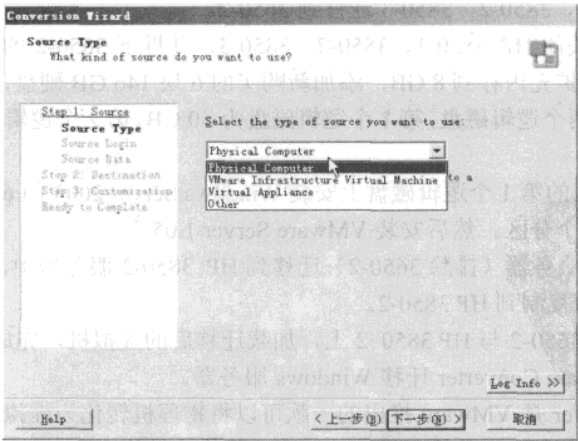


图 5-5 转换物理主机

第 5 步，在“Source Login”页中，选中“This Local machine”选项。

第 6 步，在“Source Data”页中，选择要转换的物理机上的磁盘，通常情况下，需要转换所有的磁盘。这样，转换后的虚拟机将与物理主机有相同的数据，如图 5-6 所示。

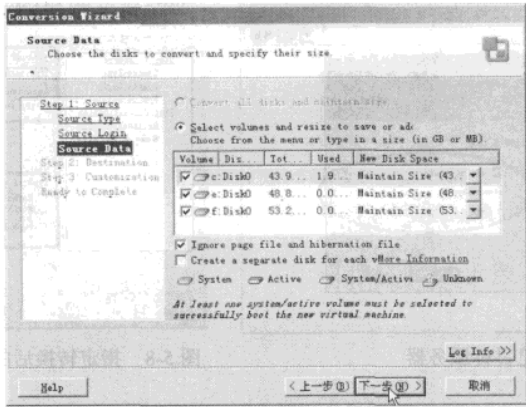


图 5-6 转换所有磁盘

第 7 步，在“Destination Type”页中，在“Select the destination type”下拉列表框中，选择“Other Virtual Machine”选项。

第 8 步，在出现“Virtual Machine Name and Location”页时，如图 5-5 所示，需要输入目标服务器的提供的共享文件夹与转换后的虚拟机的名称。在此页中暂停，然后打开“资源管理器”窗口，在“地址”栏中，以 UNC 的格式，输入远程文件服务器的 IP 地址（\\192.168.2.196），并且输入远程文件服务器的管理员账户与密码，同时选中“记住我的密码”复选框，如图 5-7 所示。然后，打开这台服务器的 D 盘共享，并打开提供虚拟机的文件夹，在本例中，为“VM_Server-VMS”，然后，在“地址”栏中“复制”这个路径（\\192.168.2.196\d\$\\VM_Server-VMS）。

第 9 步，返回到“Virtual Machine Name and Location”页中，在“Location”文本框中，“粘贴”复制的地址到列表中，然后在“Virtual machine name”文本框中，输入这台服务器的标识名称与 IP 地址，例如“IBM_3650_2-192.168.2.199”，这样做的目标是为了易于分辨，当迁移多个虚拟机时，可以根据目标，分清每个虚拟机的用途，以及是从那一台服务器迁移过来的。同时，在“Type of virtual machine to”选项组中，选择转换后的虚拟机的硬件格式，在本例中，选择 VMware Workstation 5.x 的格式，这个格式是兼容 VMware Server 1.x 的，如图 5-8 所示。

第 10 步，在“Virtual Machine Options”页中，单击“下一步”按钮。

第 11 步，在“Networks”页中，选择转换后的虚拟机中虚拟网卡的数量。在一般的物理服务器上，通常都有两块网卡，但一般情况下，只使用了其中的一块。在此，可以根据需要选择虚拟网卡的数量，通常选择 1 块即可。

第 12 步，在“Ready to Complete”页中，单击“完成”按钮，转换前的设置完成。之后，返回 VMware Converter 主界面，开始转换。

第 13 步，根据数据的大小，转换的时候可能在几分钟到几十分钟，甚至在几个小时之间，如果转换的源主机、目标主机、使用的交换机都是千兆位速度，则网卡的使用率会在 60%~90%左右；如果在这三者之间，速度不一致，例如，源主机是千兆位网卡，目标主机是百兆位

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

网卡，则源主机的网络使用率最高会在 14%左右，大部分时间会在 12%左右，如图 5-9 所示。在多次测试中，使用 VMware Converter 的转换速度大约是每分钟 470 MB~2 000 MB 左右。

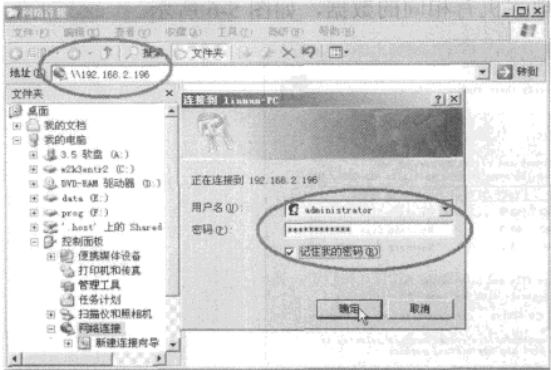


图 5-7 浏览目标服务器

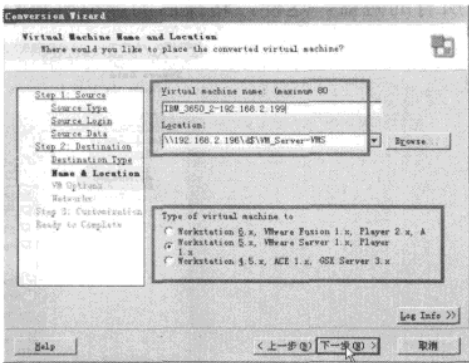


图 5-8 指定转换后的虚拟机名称及保存的路径

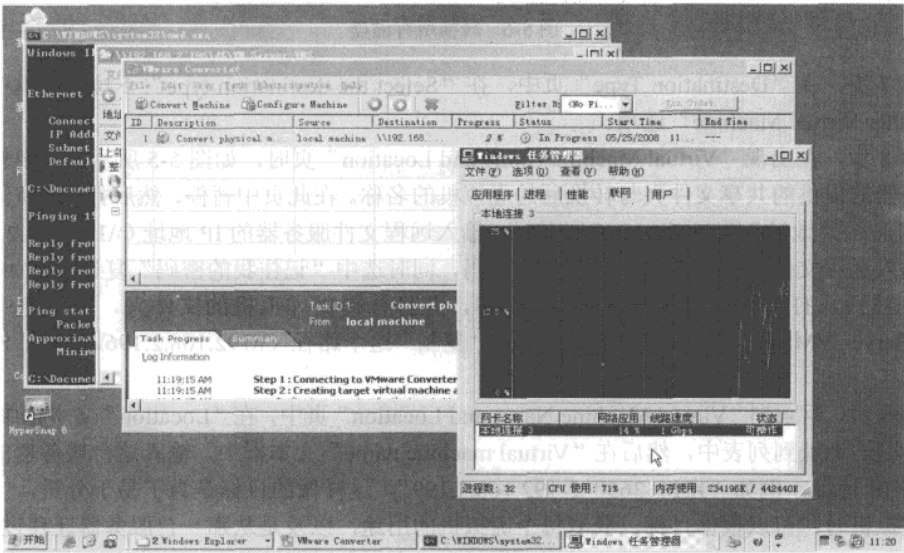


图 5-9 转换时网卡使用率

第 14 步，转换完成后，VMware Converter 进度条会显示 100%，此时关闭 VMware Converter，如图 5-10 所示，然后关闭转换的物理主机。

5. 在 VMware Server 中加载转换后的虚拟机

当把物理主机“迁移”到虚拟机后，切换到保存虚拟机镜像的服务器中，可以看到，转换后的文件夹就是图 5-8 中“Virtual machine name”文本框中指定的名称，此时，可以用 VMware Server 1.05 打开该虚拟机，可以看到，迁移后的虚拟机与原主机的配置相同：2 GB 内存、两个虚拟 CPU、显示名称为图 5-8 中指定的名称，如图 5-11 所示。这时还要根据需要进行相应的设置，迁移工作才能完成，主要步骤如下：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

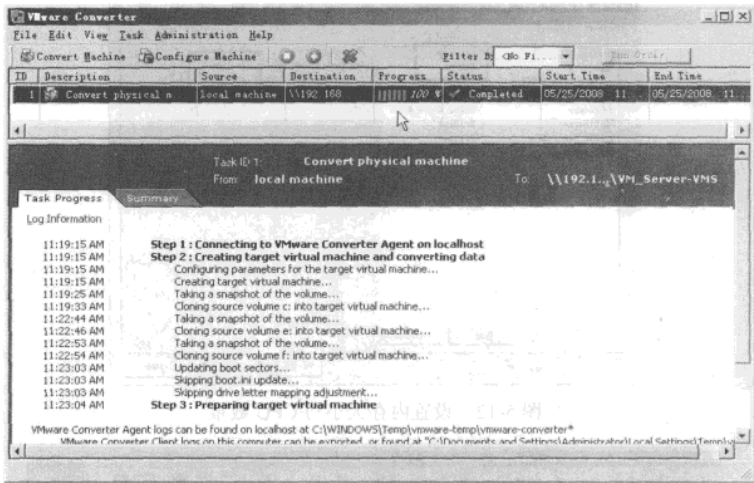


图 5-10 转换完成

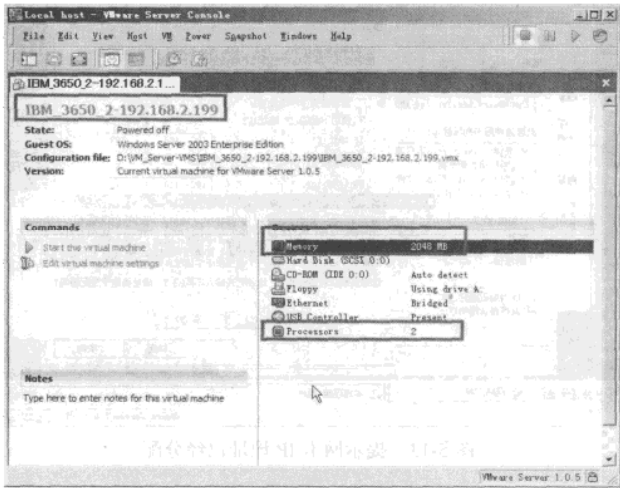


图 5-11 迁移后的虚拟机配置

- 第 1 步，修改虚拟机的设置，设置内存为实际需要大小，通常情况下，例如设置为 512 MB 大小，设置虚拟 CPU 的个数为 1，如图 5-12 所示。
- 第 2 步，在“Options”选项卡中，禁用快照，并且设置该虚拟机跟随系统启动。
- 第 3 步，然后启动虚拟机，安装 VMware Tools，设置 IP 地址为源物理主机的 IP 地址、子网掩码与网关，在设置的时候，会提示这个地址已经分配，此时单击“否”按钮即可，如图 5-13 所示。
- 第 4 步，进入“控制面板→添加或删除程序”中，删除“VMware Converter”。
- 第 5 步，检查迁移后的虚拟机中的各项服务是否已经启动，然后在网络中的其他计算机上，用以前的使用方法，访问迁移后的服务器，看提供的服务是否正常，具体的将不在这里过多介绍。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

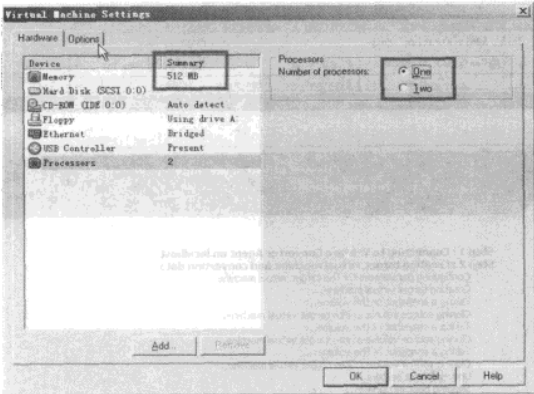


图 5-12 设置内存大小与 CPU 数量

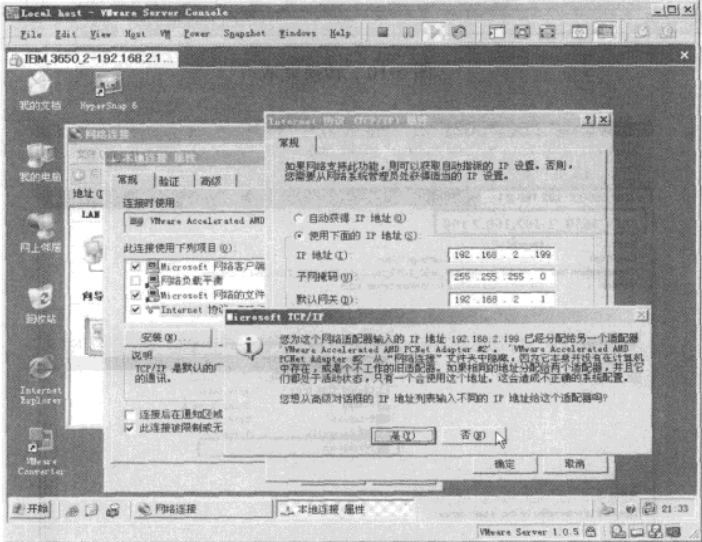


图 5-13 提示网卡 IP 地址已经分配

6. 迁移记录

在整个迁移的过程中，大约用了一天的时间，完成了所有 7 台服务器的迁移，在迁移过程中的使用经验与注意事项记录如下：

- (1) 迁移前，使用 `chkdsk c: /f`、`chkdsk d: /f`，对迁移的服务器的各个分区进行检测。
- (2) 迁移的时候，可以不关闭、不停止 SQL Server、网站等服务。可以带杀毒软件进行迁移。但是，最好把 SQL Server、网站服务停止，这样可以减少迁移的时间。
- (3) 最好删除系统中无用的软件备份(有的服务器带 SQL Server、Windows Server 2003 的安装备份)，迁移到虚拟机中，直接使用 ISO 的镜像就可以了。
- (4) 如果有多台服务器安装 SQL Server，最好另找一台主机安装 SQL Server，将迁移到虚拟机中的数据库再“迁移”到主机的 SQL Server 中，把虚拟机中的 SQL Server 卸载，这样

虚拟化应用方面 | 5

可以合理利用资源：SQL Server 集中、每个虚拟机中不用 SQL Server，虚拟机性能可以达到最好。所以，可以对应服务器，安装好每个虚拟机，将网站复制到每台虚拟机中，将 SQL Server 数据库复制到主机的 SQL Server，修改网站的配置文件、在 SQL Server 中附加一下数据库就可以了，这样就不必使用 VMware Convert，这样迁移后的主机速度最快、性能最好。

(5) 在迁移的时候，最好使用千兆位的网络。现在服务器大多是千兆位网卡。如果没有千兆位交换机，可以做一根 RJ45 直通线，在两个服务器之间迁移。在使用中，迁移 16 GB 左右的数据（带操作系统、SQL Server 数据库等），如果使用千兆位网络迁移，大约 45~90 min 即可以迁移完毕，如果是百兆位网络，大约 3 小时以上时间。

(6) 在使用 VMware Convert 迁移的时候，必须有耐心，通常从 1%~2% 很快，但系统会长时间停留在 2% 的状态，此时不要着急，多等一会（可能要等 1 个多小时），以后从 3%~100% 的时候，速度将会比较稳定。如果怀疑迁移出故障，可以去保存迁移的目标文件夹中去看一下，按 F5 刷新，如果文件持续增加，表示迁移正在进行。而且，这种情况在使用百兆位网络速度迁移时会经常出现，如果是千兆位网络，基本上不会出现这个问题。

7. VMware ACE 应用专题

这一部分我们通过两个案例，介绍 VMware ACE 在企业与个人中的应用。

(1) 迁移并分发工作站。

我们在给一些单位做网络的升级改造时，发现了一个这样的现象：在单位中，总有一些个人或部门使用的计算机，虽然已经很慢很慢了，并且只能通过“重装系统”解决，但他们却不愿意重装系统，原因也很简单，因为这些计算机上安装了一些“专用软件”，但这些专用软件的安装程序已经没有了，或者这些“专用软件”是多年前由一些计算机公司给开发的，但到了现在，开发这些软件的公司已经倒闭或者不存在了。所以即使知道这些计算机已经很难用了，但还要勉强用，因为这些计算机上还有单位的重要数据，所以，计算机即不能重装，也不能做别的用，而是像“文物”一样保护起来，否则，丢失了这些数据，单位的工作会出问题的。而且，这些计算机将来怎么办呀？万一硬盘坏了，软件怎么用，数据怎么办？

对于这种情况，作为管理员的我们大都会把整个硬盘用 ghost 备份下来，并且备份到其他计算机上，当这台计算机的硬盘坏了之后，购买新硬盘，再把系统用 ghost 恢复回来就行了，但这种方法，终究不是长久之计，而好的解决方法就是采用虚拟机。为了减轻用户的负担，可以用 VMware ACE Workstation 虚拟机，将保存有重要数据与应用软件的物理计算机迁移到虚拟机，并且打包成可执行程序，分发给用户使用。下面通过迁移一台计算机来例，介绍迁移的方法与注意事项。

① 迁移前的准备工作。

在迁移之前，要根据需要做出详细的计划，是迁移整个物理计算机上的所有硬盘、所有分区，还是只迁移保存有重要数据与应用软件的 C 盘（以前在安装软件的时候，大多都安装在了 C 盘，相应的数据也保存在了 C 盘）。为了减轻迁移后的虚拟机的大小，如果应用软件与数据都保存在了 C 盘，可以只迁移 C 盘，如果应用软件与数据保存在了其他盘，例如 D 盘、E 盘等，除了迁移 C 盘外，还要迁移保存应用软件与数据的其他磁盘，这些可以根据实际情况选择。

② 使用 VMware Convert 迁移物理机到虚拟机中。

在做好准备工作后，查看 C 盘属性。查看 C 盘使用了多少空间，这样可以大致估算，需

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

要多少空间才能完成迁移的工作，如图 5-14 所示。

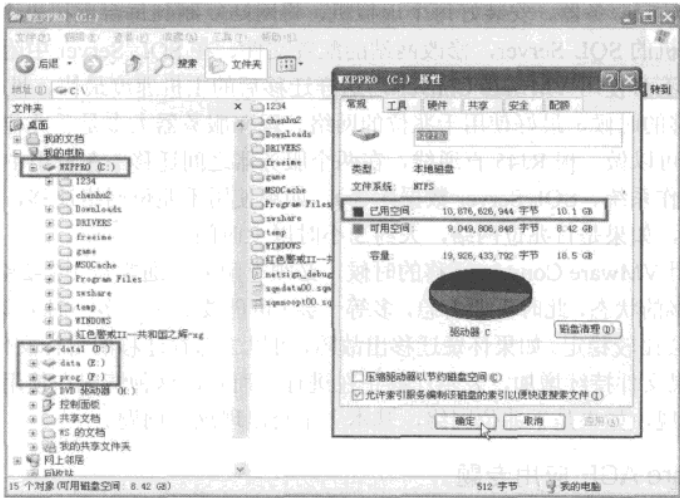


图 5-14 估算需要的空间

在估算了需要的空间后，在一个空间比较大的计算机上，通常是安装了 VMware ACE Workstation 的计算机上，创建共享文件夹（例如共享名称为 VMS），并且设置共享权限为“完全控制”，假设安装 VMware ACE Workstation 的计算机的 IP 地址是 192.168.1.80，在这台计算机上，关闭防火墙或者打开“文件和打印机共享”。然后，转到要迁移的计算机上，打开“资源管理器”，在“地址栏”中输入“\\192.168.1.80”，在弹出的对话框中，输入 192.168.1.80 计算机的管理员账户与密码，单击“确定”按钮，打开 192.168.1.80 的计算机后，打开 VMS 共享文件夹，如图 5-15 和图 5-16 所示。

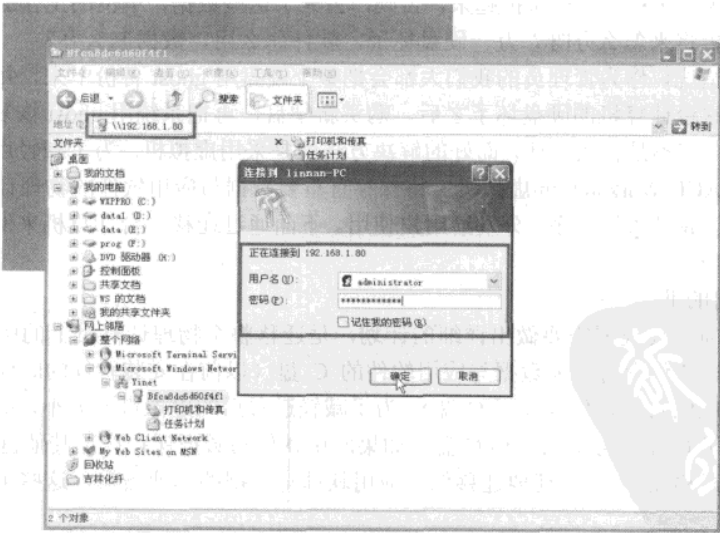


图 5-15 浏览远程计算机

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

返回到安装 VMware ACE Workstation 的计算机上（就是上面的 IP 地址为 192.168.1.80 的计算机），打开 VMware ACE Workstation，打开迁移后的虚拟机，如图 5-19 所示。

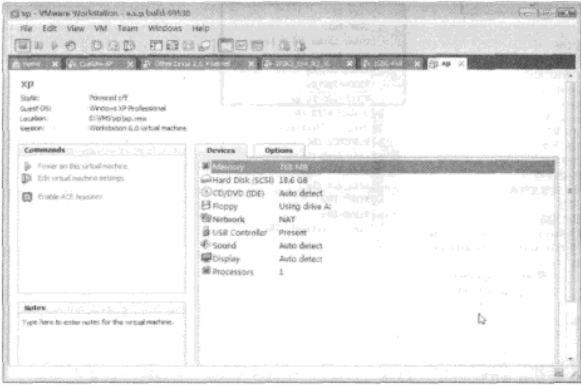


图 5-19 打开迁移后的虚拟机

首先要单击“Edit virtual machine settings”链接，修改虚拟机的内存、网卡，通常情况下，要根据目标用户的计算机为虚拟机分配内存。例如，假设迁移后的虚拟机，运行的主机只有 512 MB 内存，则为该虚拟机分配 256 MB 内存即可；如果迁移后的虚拟机其主机具有足够的内存，例如 2 GB 内存，则可以为虚拟机分配更大的内存；如果迁移的虚拟机，里面所运行的软件，不需要网络环境（有些财务软件只需要本机环境，不需要网络环境），则可以从虚拟机配置文件中“删除”网卡，这些都需要根据迁移的物理机上所安装的软件的需求进行定制。在所有的设置完成后，打开该虚拟机的电源，进入系统后安装 VMware Tools。

安装 VMware Tools 后，重启虚拟机，再次进入虚拟机后，进入“控制面板→添加删除程序”中，卸载迁移前主机系统上的驱动程序与应用软件，例如原来的显卡、声卡驱动程序如图 5-20 所示，最后再卸载 VMware Converter 程序，如图 5-21 所示。



图 5-20 卸载原来主机上的驱动程序

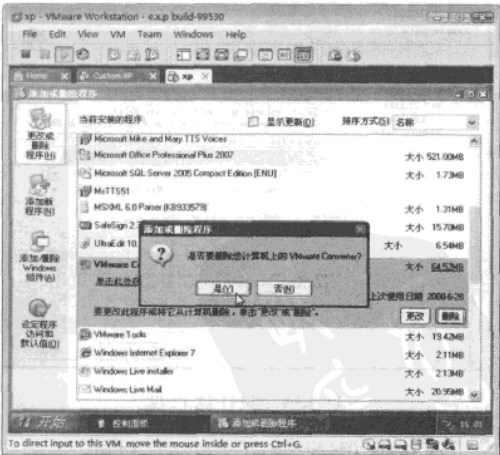


图 5-21 卸载 VMware Converter

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

在卸载掉原来主机上的驱动程序、卸载 VMware Converter 后，测试原来主机上的软件是否可用、数据是否正确，检查无误之后，关闭该虚拟机。

返回到 VMware ACE Workstation 后，启用 ACE 功能，并且使用默认的策略即可，如图 5-22 所示。

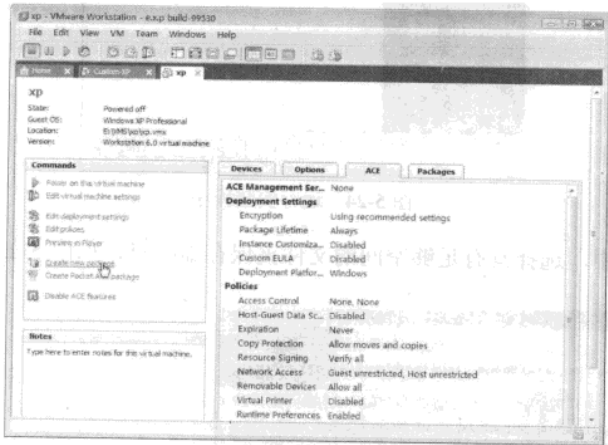


图 5-22 启动 ACE 功能

最后，在 VMware ACE Workstation 中，在“Commands”中单击“Create new package”创建 VMware ACE 包。创建 ACE 包的过程中，完全按照默认值即可。

④ 将定制好的虚拟机分发到终端。

打包之后，通过网络或者活动硬盘，将“打包”后的虚拟机，复制到用户的新计算机上，运行安装程序，安装 VMware ACE Workstation 定制的虚拟机，如图 5-23 和图 5-24 所示。

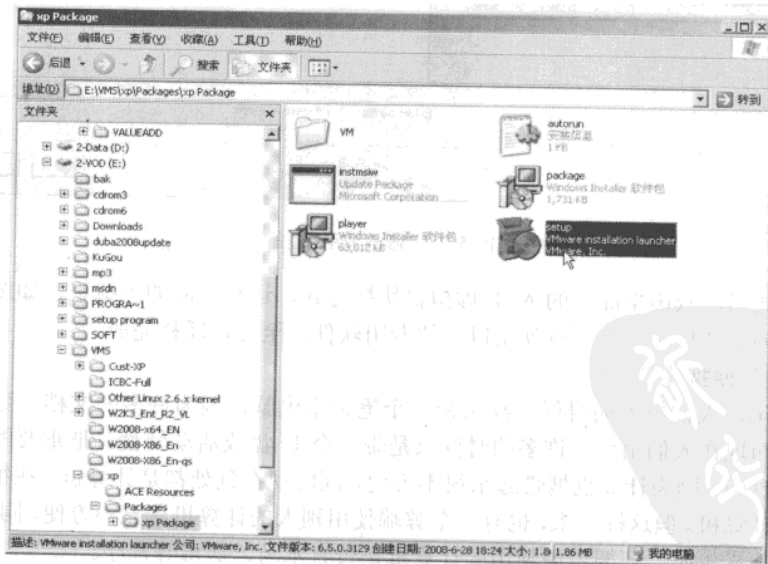


图 5-23 打包好的虚拟机

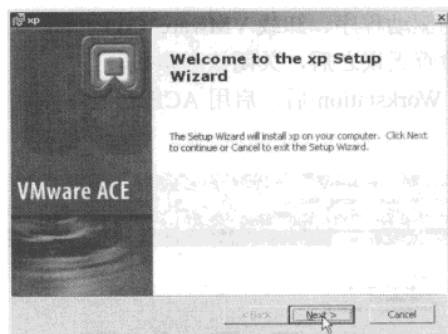


图 5-24 运行安装程序

在安装的过程中，选择具有足够空间的文件夹保存虚拟机，如图 5-25 所示。

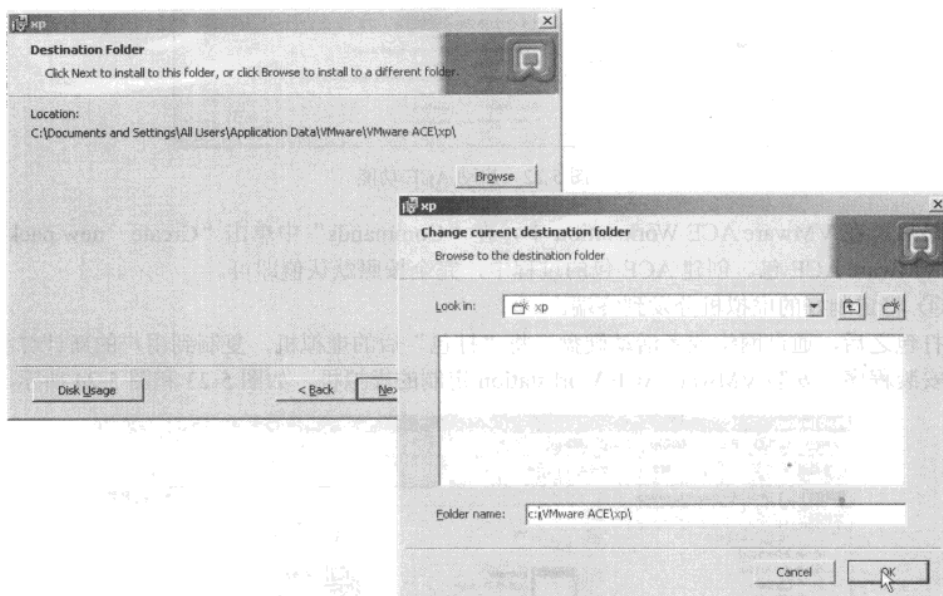


图 5-25 修改安装路径

安装完成后，双击桌面上的 ACE 虚拟机快捷方式，运行定制的虚拟机，如图 5-26 所示。以后在该虚拟机中，就可以使用以前的专用软件，至此，迁移完成。

(2) 制作便携式计算机。

在前几年，人们出差的时候，经常带一个笔记本电脑，因为许多的文档、数据都在笔记本电脑中，而现在人们出差，许多的时候只是带一个 U 盘或活动硬盘，把重要的数据放在 U 盘或活动硬盘中。因为计算机携带起来很不方便，同时现在到处都是计算机，在很多地方都能很容易找到计算机。但这样一来，也有一个弊端使用别人的计算机毕竟不方便，同时也不习惯，在网吧使用计算机时，还要考虑使用的计算机是否有木马、病毒等程序。

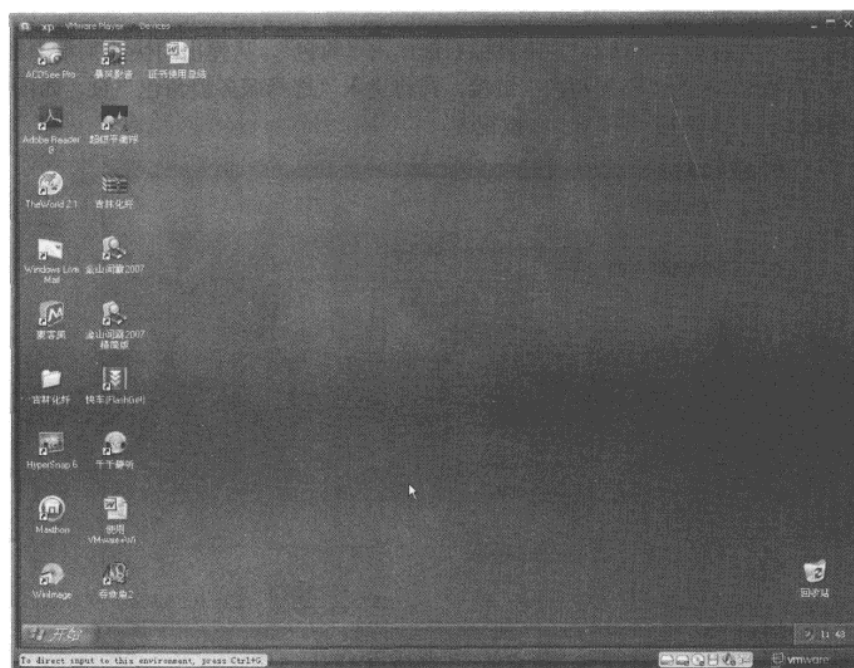


图 5-26 运行定制的虚拟机

在有了 VMware ACE Workstation 后，拥有大容量活动硬盘与 U 盘后，可以很容易定制“便携可移动”虚拟机当笔记本电脑使用，原因如下：

- ① 高速大容量设备的 U 盘或活动硬盘慢慢普及，并且价钱也越来越低。例如，2009 年 5 月份，4 GB 的 U 盘不到 100 元人民币，而 160 GB 的活动硬盘 300 元人民币左右。
- ② VMware ACE Workstation 定制的虚拟机具有高安全、高可靠性，使用简单、方便。
- ③ 人们可以随处见到计算机，例如在宾馆、网吧等，或者出差开会期间，会议主办方都会提供计算机。

■ 8. Hyper-V 使用。

Windows Server 2008 正式版发布的时候，其内置的 Hyper-V 虚拟机只是一个测试版本。在 2008 年 6 月底，Microsoft 公司发布了 Hyper-V 的正式版。在这里将介绍 Hyper-V 的使用。

（1）安装 KB950050 和 KB951636 补丁。

要在 Windows Server 2008 中启用正式版的 Hyper-V 功能，需要安装 Microsoft 提供的 KB950050 和 KB951636 补丁。在 Windows Server 2008 正式版光盘中提供的 Hyper-V 只是一个测试版。安装 KB950050 与 KB951636 补丁，与启用 Hyper-V 功能并不冲突，如果你在安装补丁之前已经启用了 Hyper-V 功能，则在更新该补丁后，Hyper-V 功能将会升级为正式版。如果先安装了 KB950050 与 KB951636 补丁，则在添加 Hyper-V 角色时，将会添加正式版的 Hyper-V。

（2）添加 Hyper-V 角色。

安装 KB950050 和 KB951636 补丁完成后（计算机需要重新启动两次），接下来要添加

网管天下 网管经验谈

Hyper-V 角色，主要步骤如下：

第 1 步，进入“服务器管理器”，用鼠标右键单击“角色”，从弹出的快捷菜单中选择“添加角色”，或者单击右侧的“添加角色”链接，都将进入“选择服务器角色”页，如图 5-27 所示，选中“Hyper-V”，然后“下一步”按钮。

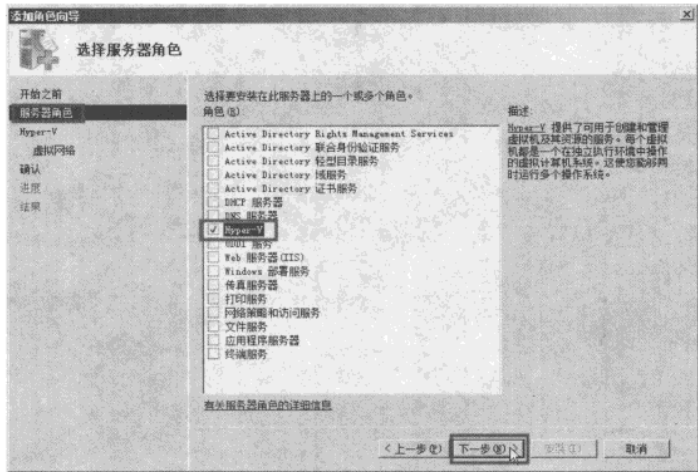


图 5-27 添加 Hyper-V

第 2 步，在“创建虚拟网络”页中，选择主机上的“以太网卡”，这将为 Hyper-V 虚拟机添加第一块虚拟网卡，如图 5-28 所示。

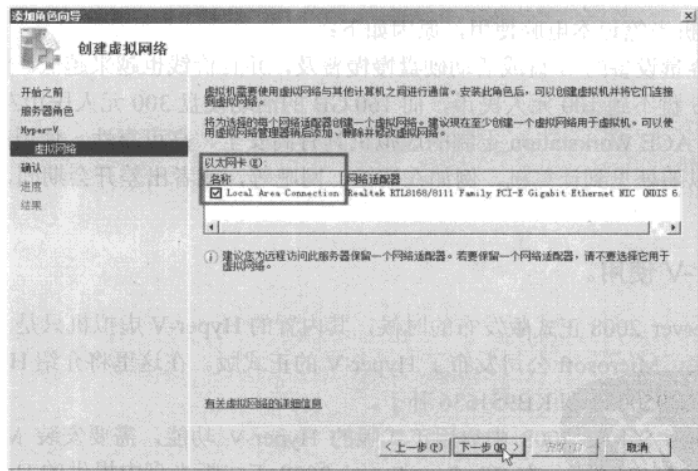


图 5-28 添加虚拟网卡

第 3 步，安装完成后，单击“关闭”按钮，在弹出的“是否希望立即重新启动”对话框中单击“是”按钮，重新启动计算机。

第 4 步，计算机重新启动两次后，完成 Hyper-V 角色的添加。

(3) Hyper-V 设置。

在“服务器管理器”中，右击计算机名称，弹出快捷菜单，如图 5-29 所示。包括“Hyper-V 设置”、“虚拟网络管理器”等命令，先选择“Hyper-V 设置”命令。

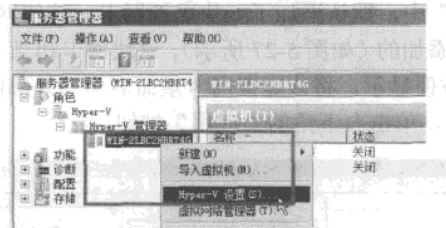


图 5-29 Hyper-V 管理器

在“Hyper-V”设置对话框中，可以设置默认的虚拟硬盘、虚拟机的保存路径、设置热键等，主要设置如下：

- ① 在“虚拟硬盘”选项中，可以设置 Hyper-V 虚拟机的虚拟硬盘默认的保存位置，在本例中，选择“c:\virtual machines”文件夹。
- ② 在“虚拟机”选项中，设置在创建虚拟机时，默认的保存位置，如图 5-30 所示，在本例中，仍然选择“c:\virtual machines”文件夹。

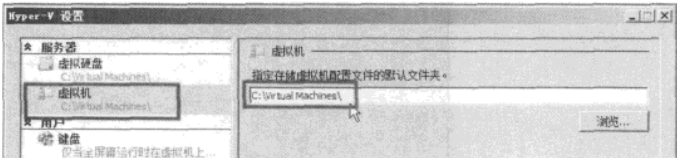


图 5-30 虚拟机保存位置

- ③ 在“鼠标释放键”选项中，设置当未运行虚拟机驱动程序时（以前称做虚拟机附加程序），怎样将鼠标从虚拟机中切换到主机中，默认为 Ctrl+Alt+向左键，可以在“释放键”下拉列表中选择，如图 5-31 所示。设置完成后，单击“确定”按钮。

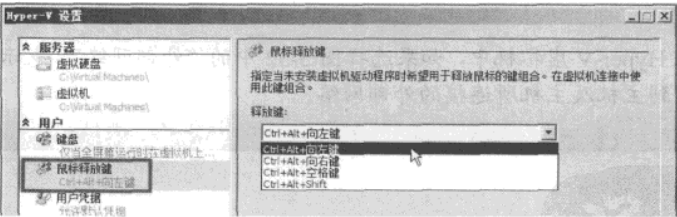


图 5-31 释放键

(4) 虚拟网络管理器。

在“虚拟网络管理器”中，可以为 Hyper-V 虚拟机添加虚拟网卡，这相当于 VMware 的“虚拟网络设置”。与 VMware 不同的是，Microsoft 的虚拟网络，没有内置 DHCP 服务器，所以在创建了虚拟网络后，如果在虚拟机中使用了这些虚拟网卡，还需要手动为虚拟机设置 IP 地址。

网管天下 网管经验谈

① 修改虚拟网络名称。

在 Hyper-V 的“虚拟网络管理器”中可以添加、删除或修改虚拟网卡，本部分先介绍修改虚拟网络名称的方法。

在“虚拟网络管理器”中，默认添加了一块虚拟网卡，这块网卡属性为“外部网络”，这是在添加 Hyper-V 角色时添加的（如图 5-27 所示）。这块网卡相当于 VMware 系列虚拟机中的 VMnet0 虚拟网卡。为了方便显示，将该虚拟网卡重命名为“外部网络”，并且添加说明文字，如图 5-32 所示。修改之后，单击右下角的“应用”按钮。

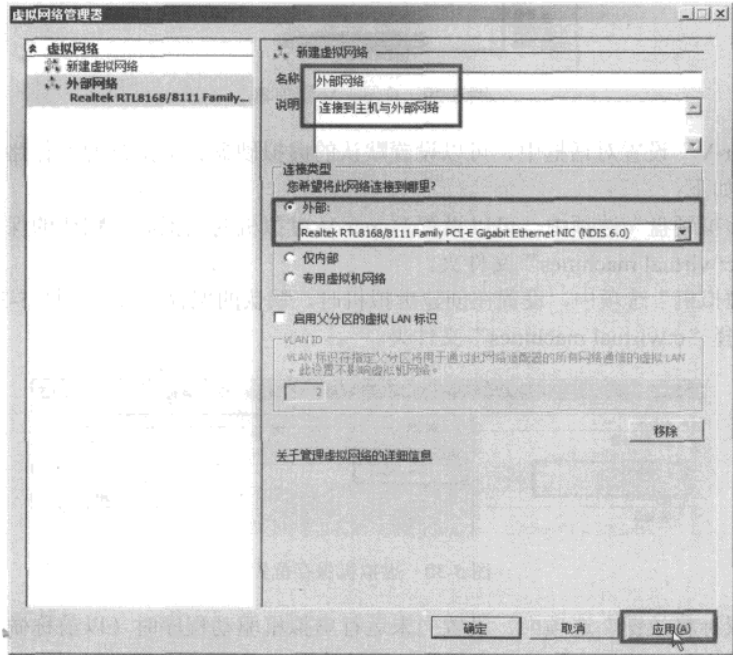


图 5-32 修改虚拟网卡名称

说·明

在 Hyper-V 虚拟机中，如果选择图 5-32 中的“外部网络”，表示该虚拟机可以连接到主机及主机所连接的外部网络。

② 添加虚拟网卡。

在 VMware 系列虚拟机中，默认情况下，VMware 添加了 VMnet1 与 VMnet8 虚拟网卡，以后当需要时，还可以添加其他的虚拟网卡。而在 Hyper-V 中，也可以添加虚拟网卡，并且其添加的虚拟网卡具有与 VMware 系列虚拟机相同或相类似的功能。其主要步骤如下：

第 1 步，在“虚拟网络管理器”页中，单击“新建虚拟网络”，在右侧的“创建虚拟网络”列表中选择“内部”，然后单击“添加”按钮。

第 2 步，在“新建虚拟网络”页中，在“名称”文本框中输入“内部网络”，在“说明”文本框中，输入针对该虚拟网络适配器的说明，在“连接类型”处选择“内部”，然后单击右

下角的“应用”按钮，如图 5-33 所示。

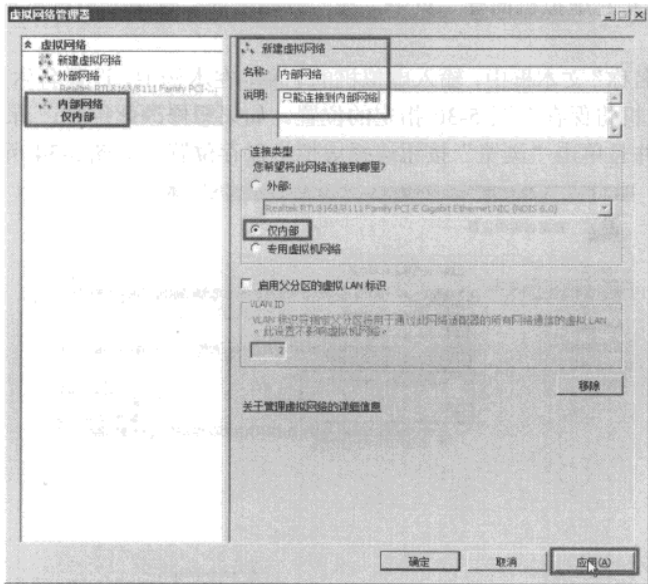


图 5-33 添加连接内部网络的网卡

说明 在 Hyper-V 虚拟机中，如果选择图 5-33 中的“内部网络”，表示该虚拟机可以连接到主机与该主机中使用“内部网络”的虚拟机。这块网卡相当于 VMnet 系列虚拟机中的“VMnet1”虚拟网卡。

第 3 步，接下来创建专门为 Hyper-V 虚拟机使用的“专用虚拟网络”。

返回到“虚拟网络管理器”，单击“新建虚拟网卡”，在“你希望创建那种类型的虚拟网络”列表中选择“专用”，然后单击“添加”按钮。

第 4 步，在“新建虚拟网络”页中，在“名称”文本框中输入“专用虚拟网络”，在“说明”文本框中，输入针对该虚拟网络适配器的说明，在“连接类型”处选择“专用虚拟网络”，然后单击右下角的“应用”按钮。

说明 在 Hyper-V 虚拟机中，如果选择刚刚创建的“专用虚拟网络”，表示该虚拟机只能连接到其他使用“专用虚拟网络”的虚拟机。这块网卡相当于 VMware Workstation 虚拟机中的“Team”中的 LAN1 等虚拟网卡。

(5) 创建虚拟机。

下面介绍在 Hyper-V 中创建虚拟机的方法。在 Windows Server 2008 中，可以在“服务器管理器”中，或者在“Hyper-V 管理器”中，创建、修改、删除虚拟机。本节以创建一个 Windows XP Professional、512 MB 内存、127 GB 虚拟硬盘、使用主机网卡的虚拟机。其主要步骤如下：

第 1 步，在“Hyper-V 管理器”中，右键单击计算机名称，从弹出的快捷菜单中选择“新

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

建——虚拟机”。

第2步，在“新建虚拟机向导”页中，在“开始之前”选中“不再显示此页”，然后单击“下一步”按钮。

第3步，在“名称”文本框中，输入虚拟机的名称，在本例中，设置名称为“Windows XP”。默认情况下，虚拟机将保存在图 5-30 指定的位置。如果想修改此位置，请选中“将虚拟机存储在其他位置”，并且单击“浏览”按钮选择虚拟机保存位置，如图 5-34 所示。

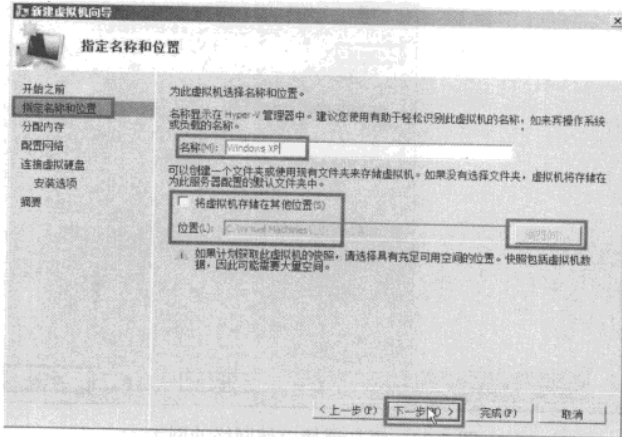


图 5-34 设置虚拟机名称与保存位置

第4步，在“分配内存”页中，为虚拟机分配内存，本例为虚拟机分配 512 MB。

第5步，在“配置网络”页中，为虚拟机选择虚拟网卡，在此选择“主机网络”。

第6步，在“连接虚拟硬盘”页中，为虚拟机创建虚拟硬盘。在此可以设置虚拟硬盘名称、虚拟硬盘保存位置以及虚拟硬盘大小。

第7步，在“安装选项”页中，选择安装操作系统的方法。在本例中，选择从 Windows XP 安装光盘镜像安装，如图 5-35 所示。

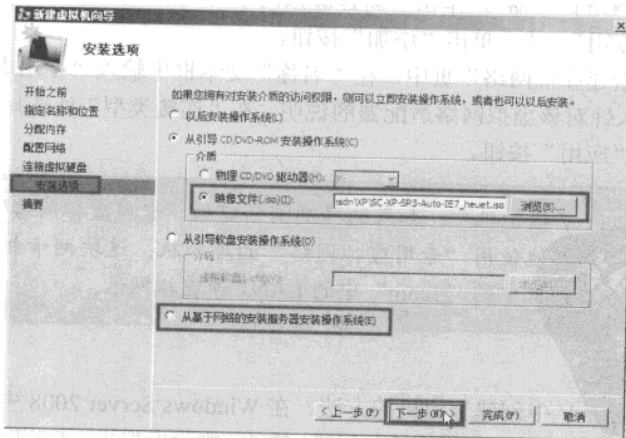


图 5-35 安装操作系统的方法

第8步，创建虚拟机完成，如果想立刻启动虚拟机，则选中“创建之后启动虚拟机”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(6) 在虚拟机中安装操作系统。

启动虚拟机后，在虚拟机中安装操作系统则比较简单。现在看一下 Hyper-V 虚拟机的界面，如图 5-36 所示。

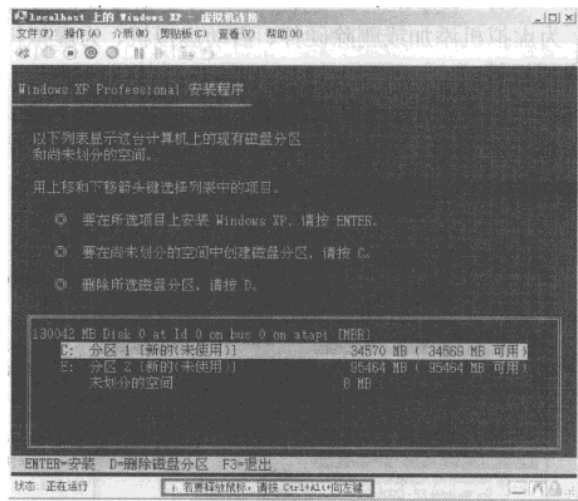


图 5-36 Hyper-V 界面

在图 5-36 最下一行显示“若要释放鼠标，请按 Ctrl+Alt+向左键”，这相当于 VMware 中的 Ctrl+Alt 组合键，就是从虚拟机中返回到主机的热键。

安装操作系统后，从“操作”菜单选择“插入集成服务安装包”，这在 VMware 中相当于安装 VMware Tools，在 Virtual PC 与 Virtual Server 中，相当于“附加程序”，也就是一些集成了驱动程序和其他一些虚拟机的增强程序而已，如图 5-37 所示。

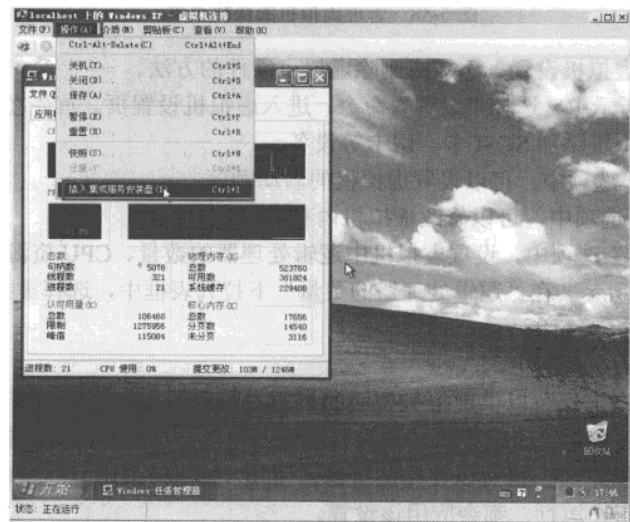


图 5-37 安装附加程序

网管天下 网管经验谈

安装完成之后，单击“是”按钮，重新启动虚拟机。之后，从虚拟机到主机就不需要热键，可以直接用鼠标来回切换了。

(7) 管理虚拟机。

在“服务器管理器”或者“Hyper-V 管理器”中，可以很方便的对虚拟机进行管理，这包括修改虚拟机的配置、为虚拟机添加或删除硬件、启动虚拟机、为虚拟机创建快照、从快照还原、重命名或者删除虚拟机等。

进入“服务器管理器”或者“Hyper-V 管理器”中，在右侧的“虚拟机”列表中，选中想要管理的虚拟机，用鼠标右键单击，就会弹出虚拟机管理的快捷菜单，如图 5-38 所示。

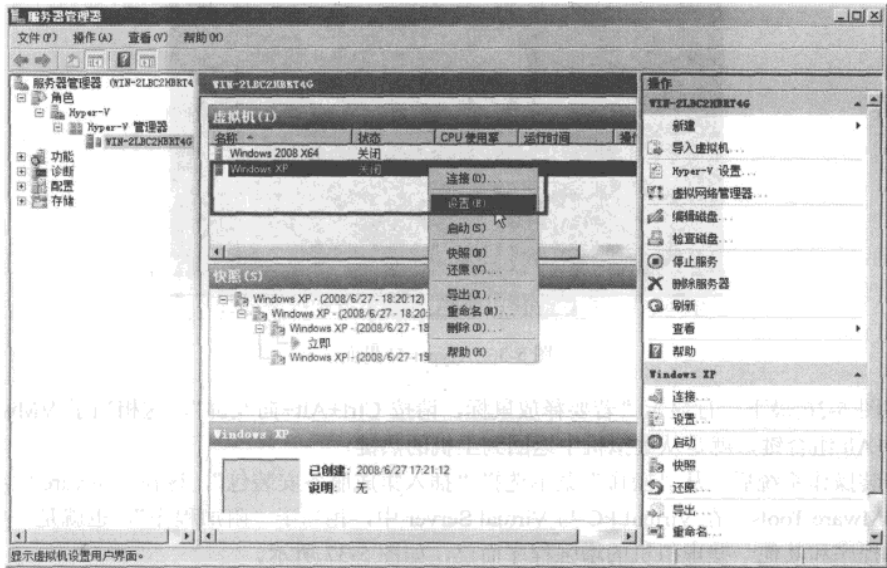


图 5-38 管理虚拟机的快捷菜单

首先介绍修改虚拟机设置、添加或删除虚拟机硬件的方法。

① 在图 5-38 所示中，选择“设置”命令，进入虚拟机设置页。首先在“添加硬件”选项中，可以为当前虚拟机添加 SCSI 卡、网卡等设备。

② 在“BIOS”选项中，可以设置虚拟机的启动顺序。

③ 在“内存”选项中，可以修改虚拟机内存的大小。

④ 在“处理器”选项中，设置虚拟机中逻辑处理器的数量、CPU 资源控制、处理器功能等设置，如图 5-39 所示。在“逻辑处理器的数量”下拉列表框中，选择虚拟机 CPU 数量，可以选择 1~2。

在“资源控制”选项组中。

虚拟机保留：指定保留以供虚拟机使用的资源占可用于虚拟机的所有资源的百分比。该设置保证将指定的百分比用于虚拟机。该设置还影响可以一次运行的虚拟机数量。

虚拟机限制：指定虚拟机可以使用的资源占可用于虚拟机的所有资源的最大百分比。无论是否其他虚拟机正在运行，都会应用该设置。

相对权重：指定当多个虚拟机正在运行并且虚拟机竞争资源时，Hyper-V 为该虚拟机分

配资源的方式。

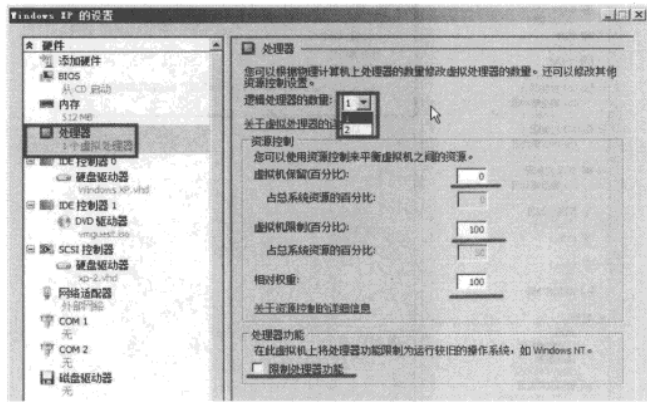


图 5-39 处理器选项

如果该虚拟机要安装（或运行）Windows NT 等比较旧的操作系统，可以选中“限制处理器”功能选项。

⑤ 在“自动启动操作”选项中，设置虚拟机自动启动选项，如图 5-40 所示。

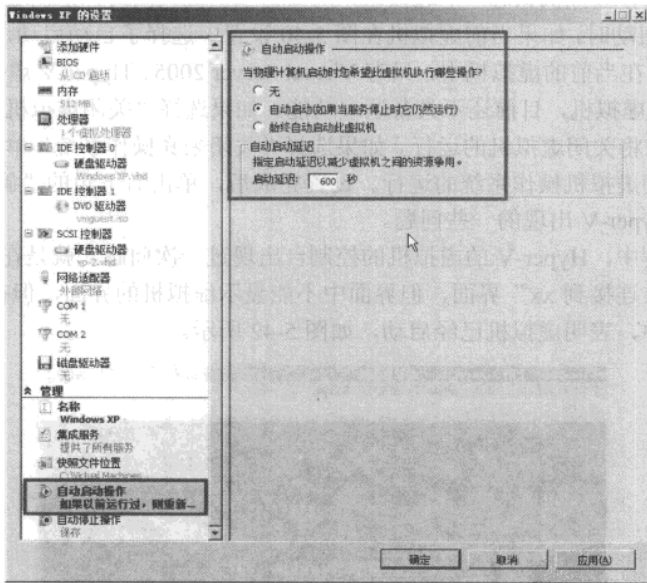


图 5-40 自动启动操作

如果希望当前虚拟机可以在物理主机启动后，自动启动该虚拟机，则可以选择“自动启动”或“始终自动启动此虚拟机”单选按钮。如果有多台虚拟机需要自动启动，可以为每台虚拟机设置“启动延迟”，以减少虚拟机之间的资源争用。

⑥ 在“自动停止操作”选项中，设置物理计算机关闭时，虚拟机执行的操作，如图 5-41 所示。

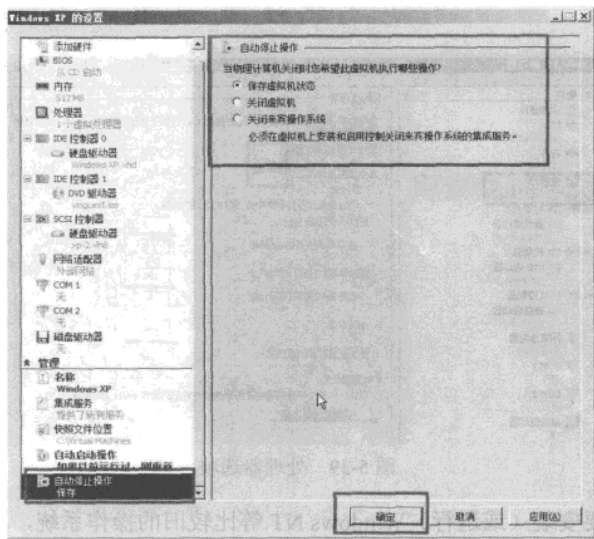


图 5-41 自动停止操作

如果选择“保存虚拟机状态”单选按钮，则当物理主机关闭时，正在运行的虚拟机会“休眠”；当物理主机启动时，如果当前虚拟机在图 5-40 设置中选择了自动启动，该虚拟机会从“休眠”状态中恢复。在当前的虚拟机中，只有 Virtual Server 2005、Hyper-V 虚拟机提供了该项功能，VMware 系列虚拟机，目前还不具备这项功能。如果选择“关闭虚拟机”单选按钮，则当物理主机关闭时，将关闭虚拟机的运行。如果选择“关闭来宾操作系统”单选按钮，当物理主机关闭时，将关闭虚拟机操作系统的运行。设置完成后，单击右下角的“确定”按钮。

（8）使用 Hyper-V 出现的一些问题。

在使用的过程中，Hyper-V 的虚拟机的控制台出现过一次问题，就是在启动虚拟机之后，一直停留在“正在连接到 xx”界面，但界面中不能显示虚拟机的界面，但在 Hyper-V 的控制台中的预览界面中，表明虚拟机已经启动，如图 5-42 所示。

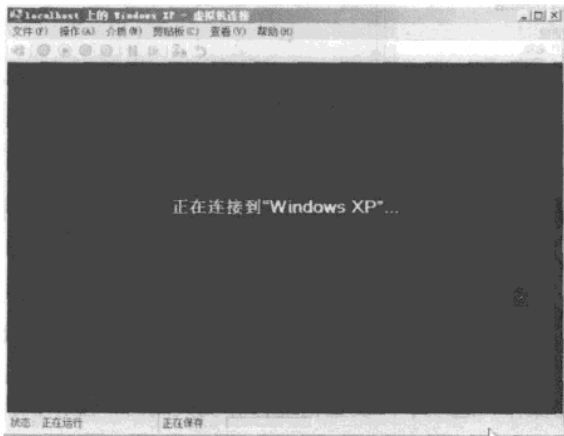


图 5-42 一直停留在此界面

最后，重新启动了 Hyper-V 的服务之后，图 5-42 中才正常显示出了虚拟机的界面。

Hyper-V 的虚拟机其热键是 Ctrl+A、Ctrl+R 等，这些热键不能修改，并且 Ctrl+Alt+Del 仍然用 Ctrl+Alt+End 代替，这与终端服务中的 Ctrl+Alt+Del 相冲突。但这一切都不会影响 Hyper-V 的使用。总体来说，Hyper-V 性能与 VMware Workstation、VMware GSX Server、VMware Server 相近，另外还具有 VMware GSX Server、VMware Server 所不具有的一些功能，加上与 Windows 产品良好的兼容性，相信 Hyper-V 在未来的虚拟化市场中会占有一席之地的。

5.1.2 | 证券公司 Netware 服务器故障解决方案

某证券公司的 Netware 4.11 服务器硬盘出现问题——在收盘的时候用了 3 个多小时，这在以前只需要 10 分钟左右的时间。因为这台服务器已经使用多年了，考虑可能是硬盘使用太频繁才出的故障。所以准备更换一台服务器，一开始考虑购买一台 HP、IBM 或者联想、方正的“品牌”服务器，但从这些公司的网站上了解到，现在的服务器已经不支持 Netware 4.11 了。又直接联系了这些公司的技术人员，相关的人员告知：现在的服务器可以支持 Netware 5.0、6.0，但不保证支持 Netware 4.11。最后只有组装一台高档的计算机或者服务器来安装 Netware 4.11。

首先使用当前使用的普通 PC 机安装 Netware 4.11，在进入安装屏幕后死机。重新组装了一台服务器，安装时仍然死机。后来，把在虚拟机中安装好的 Netware 4.11 使用 ghost 克隆下来，将其“克隆”到服务器后可以使用，但在加载服务器的网卡驱动程序时（已经进入 Netware 4.11），无法加载（因为网卡提供的是 Netware 5.0 的驱动）。经过多次尝试后，直接在物理计算机上安装 Netware 4.11 不能成功。原因可能有两个：一是当前计算机都是 64 位的处理器。Netware 4.11 是 1995 年左右的产品，当时主流是 16 位和 32 位的平台。二是现在的计算机网卡、SCSI、RAID 卡，一般不提供 Netware 4.11 的驱动程序。

说·明

Netware 的安装实际很简单，只要能加载网卡与硬盘驱动即可。

最后，决定使用——虚拟机。正好前几天买了一台高档的计算机用来做实验，在这台计算机上安装好虚拟机后，带到证券公司，进行了下面的迁移工作。

（1）在主机上安装 Windows Server 2003，然后安装 VMware Server。

（2）将主机的 IP 地址设置为 10.1.1.1，子网掩码设置为 255.0.0.0，保存 D 盘有足够的空间，如果 D 盘是光驱盘符，在“计算机管理”中修改光驱盘符，并将其他分区修改为 D。

（3）在主机上安装“MaxDOS 5.6 PXE 镜像版”，安装完成后，打开“GhostCast Server 8.3”界面，在“会话名称”文本框中输入“max”，选择“创建映像”单选按钮，在“映像文件”中单击“浏览”按钮，将创建的镜像保存在 D 盘上，并命名为 nw411.gho，选中“磁盘”单选按钮，设置完成后，单击“接受客户机”按钮，如图 5-43 所示。

（4）切换到原 Netware 4.11 服务器上，将该服务器的网线与 Windows Server 2003 主机网络接在同一个交换机上，关闭并重启 Netware 4.11 服务器，进入 CMOS 设置，设置该服务器网卡引导（使用 PXE 方式）。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

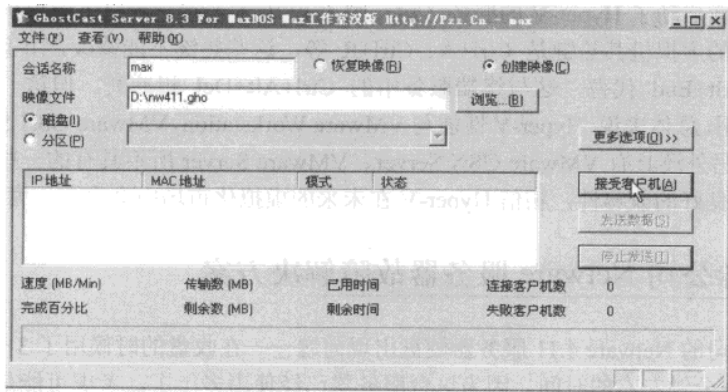


图 5-43 创建影像

说明

一般的服务器都支持 PXE 的引导，即使服务器是上个世纪的产物。如果你的服务器不支持 PXE 的引导，可以下载 MaxDOS 的光盘版，然后刻录光盘并用该光盘启动服务器，其使用方法与下面相同。

从 PXE 引导后，会从 Windows Server 2003 中下载引导文件，在启动后，选择第 2 项“使用 NDIS 网卡驱动全自动网刻”，如图 5-44 所示。

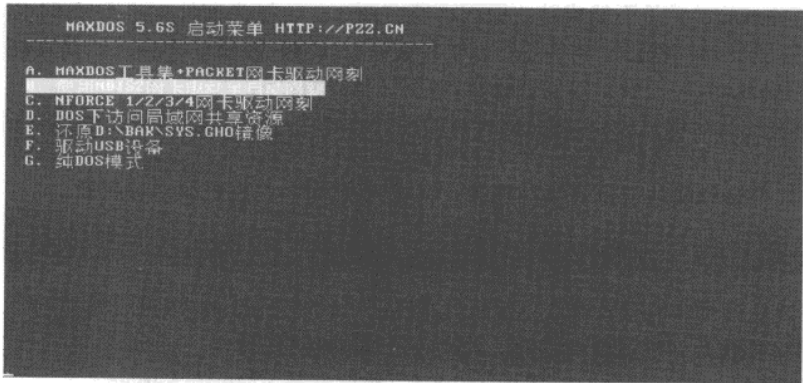


图 5-44 使用 NDIS 网卡驱动全自动网刻

说明

如果你的服务器不能出现图 5-44 所示的菜单，而是显示“显示器超出频率范围”，则按一下下箭头光标键，即“↓”，然后按 Enter 键，将会继续。

在“MaxDOS NDIS2 驱动全自动网刻系统”页中，选择第 3 项“备份镜像至服务器”，如图 5-45 所示。在下一个界面中选择备份全盘，输入 A 并按 Enter 键，如图 5-46 所示。

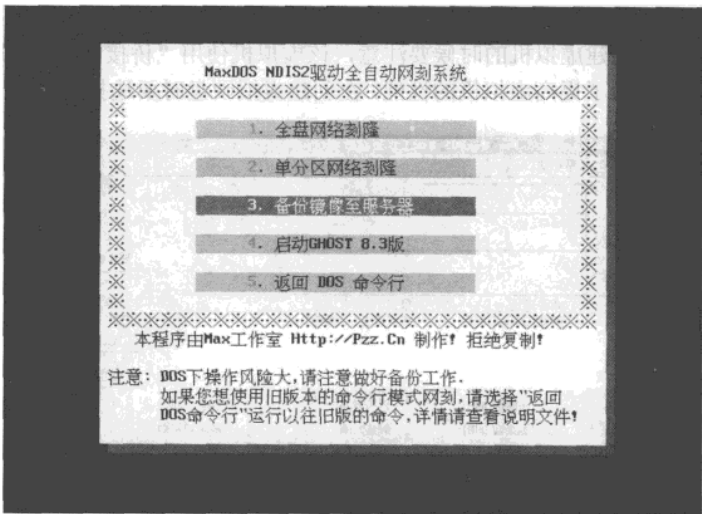


图 5-45 备份影像至服务器

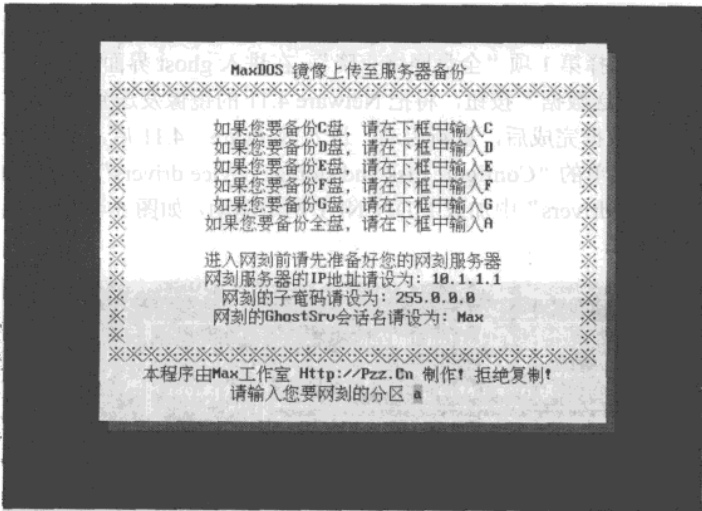


图 5-46 备份全盘

启动 ghost 并将该服务器上的硬盘所有数据上传到 Windows Server 2003 的 ghost server 中去。

(5) 上传完成后，关闭 Netware 服务器。

(6) 返回到 Windows Server 2003 主机，修改 ghostcast server，将“创建映像”改为“恢复映像”，其他保持不变，然后单击“接受客户机”按钮，如图 5-47 所示。以后的操作都将在主机中进行。

(7) 运行 VMware Server，创建 Netware 6 的虚拟机，创建虚拟机硬盘为 IDE 接口，硬盘大小与原 Netware 4.11 服务器硬盘使用的卷大小接近或者略微大于原来的卷。例如，作者克隆的这台 Netware 4.11，本来是一块 60 GB 大小的硬盘，但只创建了一个 1 GB 的主 DOS 分区(启

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

动 Netware 4.11 用)，和一个 7 GB 多的 SYS 卷，那么只需要创建一个 10 GB 的 IDE 接口的虚拟硬盘就可以了。在创建虚拟机的时候要注意，该虚拟机使用“桥接网卡”，虚拟机内存使用 256 MB 即可。另外，为了提高虚拟机的性能，在创建虚拟硬盘时要选择“立刻分配硬盘空间”。

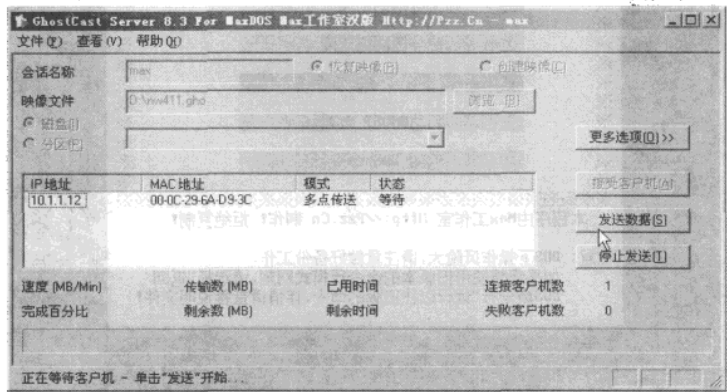


图 5-47 恢复映像

(8) 启动该虚拟机，并使用 PXE 网卡启动，在出现图 5-44 所示的菜单时选择第 2 项，在出现图 5-45 所示时选择第 1 项“全盘网络克隆”。在进入 ghost 界面后，返回到 ghost server 中如图 5-47，单击“发送数据”按钮，将把 Netware 4.11 的镜像发送到虚拟机中。

(9) 虚拟机接收数据完成后，重新启动。进入 Netware 4.11 后，使用 load install 命令，在“Driver Options”菜单的“Configure disk and storage device drivers”中加载 IDE 硬盘驱动，在“Configure network drivers”中加载 MDPCNET 网卡驱动，如图 5-48 所示。加载 IDE 硬盘驱动后，激活 SYS 卷。

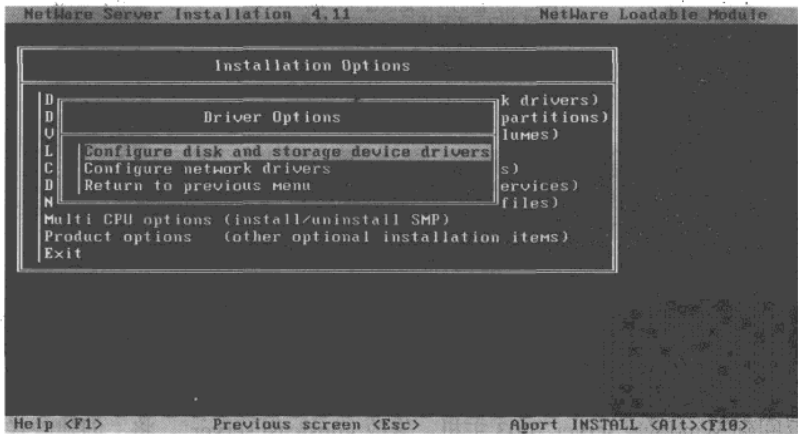


图 5-48 加载硬盘和网卡驱动

(10) 打开 load install 界面，在“NCF files options”中，编辑启动脚本（分别选择“Edit autoexec.ncf”和“Edit startup.ncf file”），将里面的原来的硬盘驱动及网卡驱动分别替换为 IDE 与 PCNTNW，然后保存退出，如图 5-49 所示。

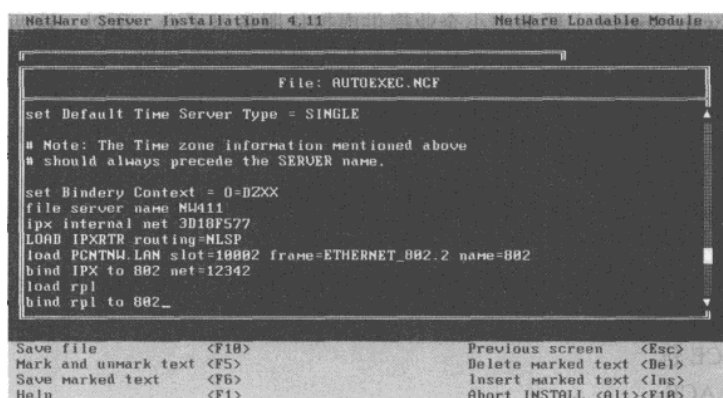


图 5-49 编辑启动脚本

说
明

不要“创建”脚本，而是“编辑”脚本。

(11) 使用 `down` 与 `exit` 命令退出 Netware 4.11，并再次进入，然后启动原来的所有无盘工作站，登录进入。

(12) 测试完毕后，关闭 Netware 4.11 虚拟机（先使用 `down`、`exit` 命令返回到 DOS 界面后，再关闭虚拟机电源），修改 Netware 4.11 虚拟机的配置，让其在系统启动时自动加载。

5.1.3 轻松打造潜行者活动硬盘电脑

某次从北京回家，在动车提供的杂志中看到“潜行者活动硬盘电脑”的广告，主要意思是：在活动硬盘上提供个人专用的、安全的“计算机”，而带“计算机”的这个活动硬盘大约卖 2800 多元钱。

实际上，可以使用 VMware ACE Workstation，在活动硬盘甚至是 U 盘上，创建这种便携式的计算机，潜行者活动硬盘也是使用 VMware 实现的。在活动硬盘或 U 盘上定制虚拟机，是有现实意义的。

基于此，在活动硬盘或 U 盘上部署经过加密的可移动计算机是非常实用的事情。在本节中，将在一个 4 GB 的 U 盘上，部署一个虚拟硬盘为 3.5 GB 大小的、安装 Windows XP Professional 的虚拟机，当需要使用的时候，直接将 U 盘插到计算机上，运行 U 盘中的 VMware Player 程序就可以使用。

(1) VMware ACE Workstation 使用规则。

VMware ACE 中的“ACE”是 Assured Computing Environment 的简称，它用来提供安全、基于策略进行管理的虚拟 PC 环境的平台。VMware ACE 可以作为一个独立平台使用，也可以和 VMware Workstation 6 结合使用。

VMware Workstation 主要为开发人员、网络管理员、技术爱好者等专业人员，提供测试与

网管天下

网管经验谈

实验环境，VMware Server 主要为中小企业提供虚拟化服务器平台，所以，这两个产品的用户都是“专业”人员，而 VMware ACE 是由“专业人员”定制虚拟机，定制的虚拟机是给普通用户使用。

下面以在一个 4 GB 的 U 盘上创建一台 Windows XP 虚拟机为例，介绍 VMware ACE 定制虚拟机的方法，大概步骤如下。

- ① 在 VMware Workstation 中创建虚拟机，在虚拟机中安装操作系统、VMware Tools、安装应用软件。
- ② 在 VMware ACE Workstation 对安装配置好的虚拟机“启用”ACE 功能。
- ③ 编辑 ACE 策略。
- ④ 创建 ACE 包。
- ⑤ 并部署 ACE。
- ⑥ 最终用户使用。

(2) 在 VMware Workstation 中创建虚拟机并启用 ACE 功能。

首先，在 VMware Workstation 中，创建 Windows XP Professional 的虚拟机，主要步骤如下。

第 1 步，运行 VMware Workstation，执行“File”→“New”→“Virtual Machine”命令，进入创建虚拟机向导，如图 5-50 所示。直接按“Ctrl+N”组合键同样进入创建虚拟机向导。

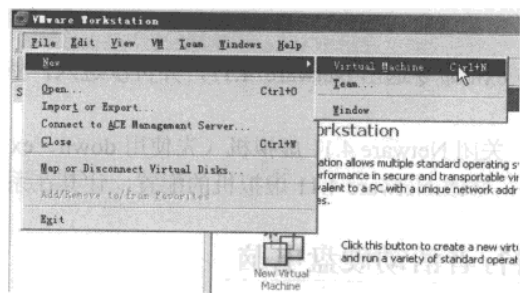


图 5-50 进入创建虚拟机向导

第 2 步，在“Welcome to the New Virtual Machine Wizard”页中，选择虚拟机的硬件格式，在此选择“Typical”的格式，如图 5-51 所示。

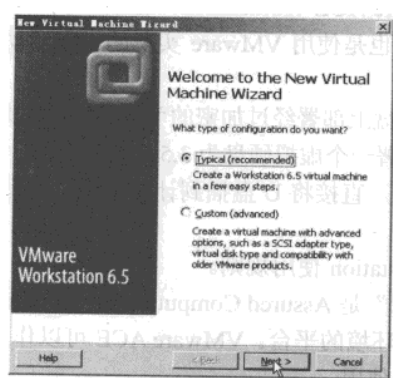


图 5-51 选择硬件格式

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

第 3 步，在“Guest Operating System Installation”页中，选择“I will install the operating system later”单选按钮，如图 5-52 所示。

第 4 步，在“Select a Guest Operating System”对话框中，选择“Windows XP Professional”操作系统，如图 5-53 所示。

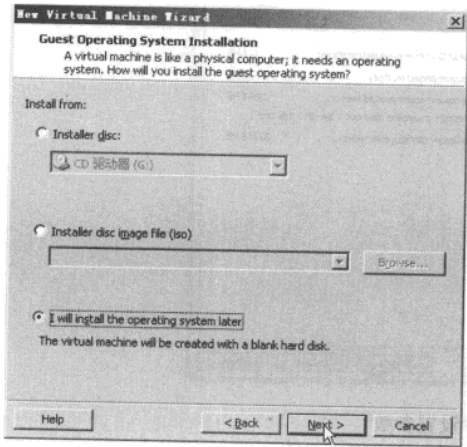


图 5-52 选择 “I will install the operating system later” 单选按钮

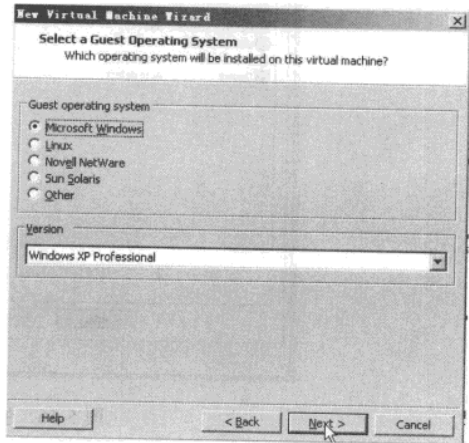


图 5-53 选择要装的操作系统版本

第 5 步，在“Specify Disk Capacity”页中设置虚拟磁盘大小，在此设置为 3.5 GB，如图 5-54 所示，单击“Next”按钮。

第 6 步，在“Ready to Create Virtual Machine”页中，可以查看其他虚拟硬件的设置信息，如图 5-55 所示。单击“Finish”按钮，将完成新建虚拟机的设置情况。

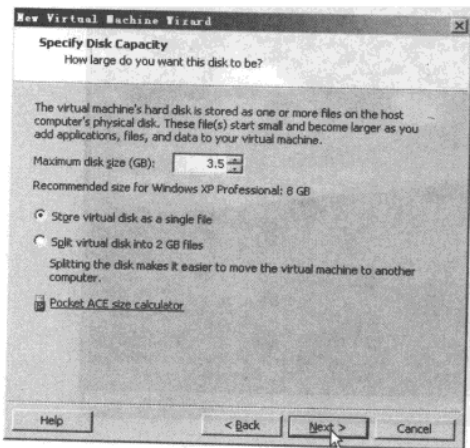


图 5-54 设置虚拟硬盘大小

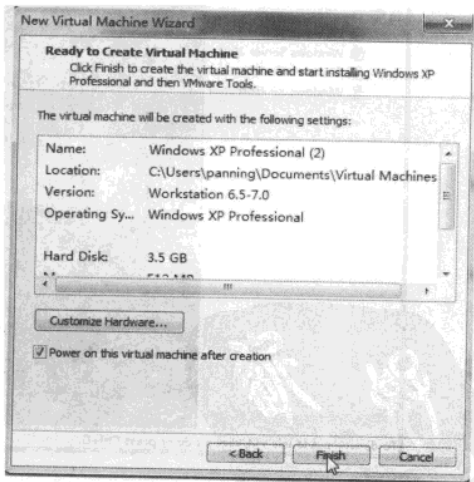


图 5-55 核对设置信息

第 7 步，如果对自动设置的其他参数不满意，在图 5-55 所示中单击“Customize Hardware...”按钮，将进入“Hardware”的设置页，如图 5-56 所示可以对虚拟机的其他参数进行修改。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

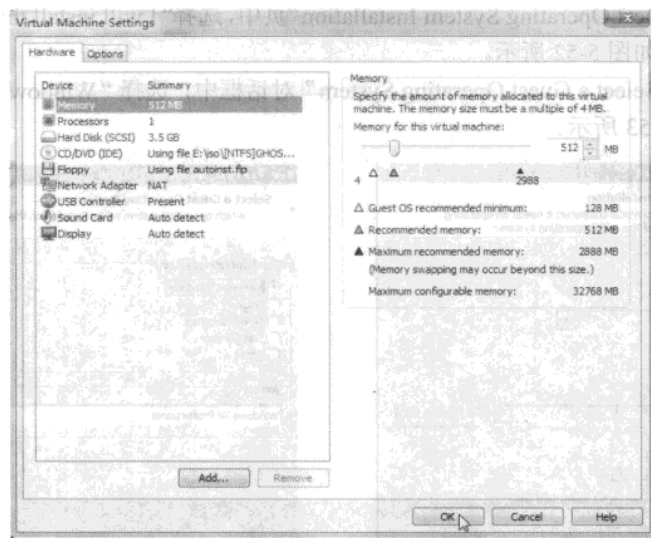


图 5-56 修改硬件设置参数

第 8 步，创建完虚拟机后，就可以在虚拟机中安装操作系统。最后安装 VMware Tool、安装所需要的软件，如 QQ，虚拟光驱等，如图 5-57 所示。



图 5-57 虚拟机系统

第 9 步，安装完成后，关闭虚拟机。在 VMware Workstation 主界面中，单击“Enable ACE features”链接，如图 5-58 所示，启用 ACE 功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

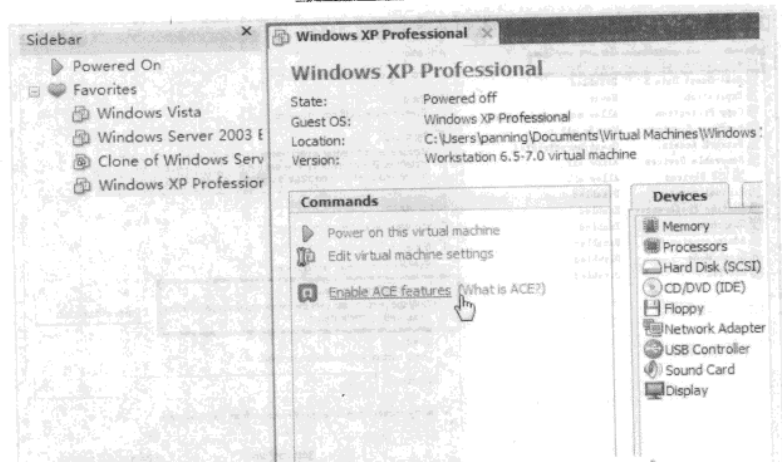


图 5-58 启用 ACE 功能

(3) 设置策略。

在启用 ACE 功能后，单击“Edit Policies”链接，如图 5-59 所示，进入 VMware ACE 策略页。

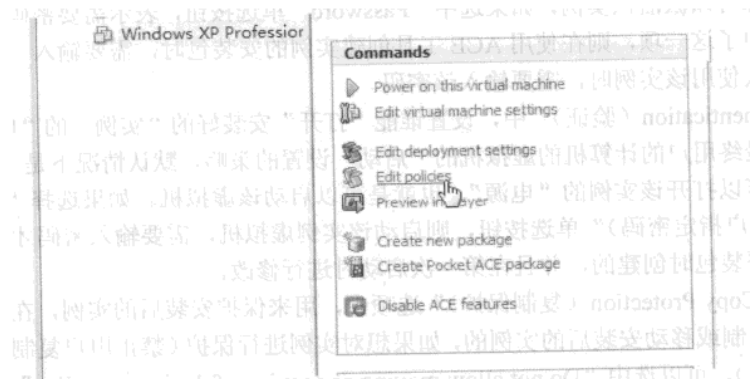


图 5-59 编辑 ACE 设置

① 在“访问控制”策略中，选择“User-specified password”单选按钮，这样部署到 U 盘中的虚拟机每次启动前都需要密码，就可以防止非授权用户使用，如图 5-60 所示。

说·明

在“Access Control（访问控制）”选项组中，可以对 VMware ACE 的“实例”的激活、打开该“实例”的电源进行控制。首先介绍一下“实例”，在 VMware ACE Workstation 中，“实例（instances）”指的是一个安装好操作系统、应用程序的虚拟机，除了指正在设置的这台“模板”虚拟机，还包括了将定制的虚拟机分发后，安装到最终用户计算机上的虚拟机，当然，安装到最终用户计算机上的虚拟机是“模板”计算机的一个复制样本。理解了实例的意义之后，就可以继续介绍“Access Control（访问控制）”策略了。

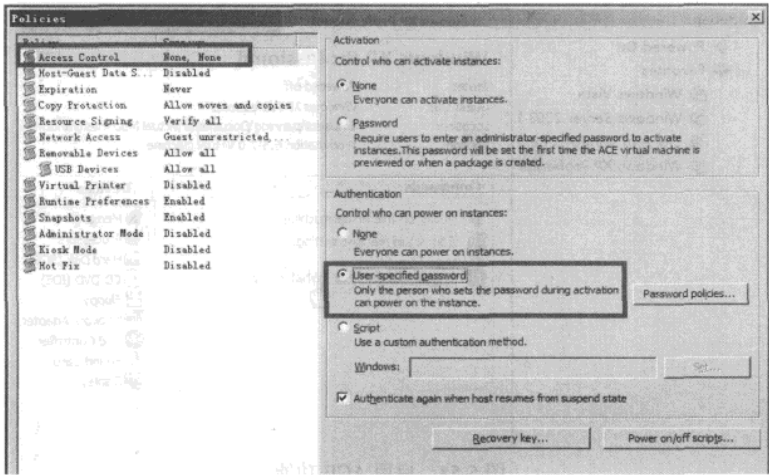


图 5-60 使用指定密码才能启动 ACE 实例

在“Access Control（访问控制）”中，包括“Activation（激活）”、“Authentication（验证）”两项，在“Activation（激活）”选项中，可以设置谁可以激活这个实例，默认是“None”设置，表示任何人都可以激活该实例，如果选中“Password”单选按钮，表示需要密码才能激活该实例。如果选中了这一项，则在使用 ACE 工具创建实例的安装包时，需要输入一个密码，并且用户在第一次使用该实例时，需要输入该密码。

在“Authentication（验证）”中，设置谁能“打开”安装好的“实例”的“电源”，该设置是对安装到最终用户的计算机的虚拟机的“启动”设置的策略，默认情况下是“None”，表示所有用户都可以打开该实例的“电源”，也就是可以启动该虚拟机。如果选择“User-specified password（用户指定密码）”单选按钮，则启动该实例虚拟机，需要输入密码才可以，而该密码是在创建安装包时创建的，并且在第一次启动时进行修改。

② 在“Copy Protection（复制保护）”选项中，用来保护安装后的实例，在默认情况下，是允许用户复制或移动安装后的实例的，如果想对实例进行保护（禁止用户复制或移动安装好的虚拟机实例），可以选中“Do not allow moving or copying of the instance files”单选按钮，如图 5-61 所示。

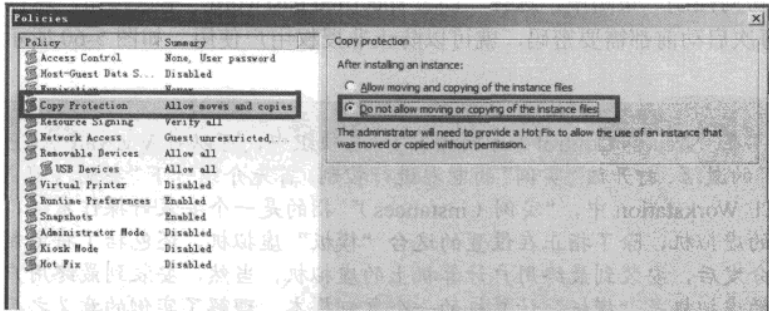


图 5-61 不允许复制或移动实例

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

- ③ 在“Virtual Printer（虚拟打印机）”控制策略中，可以决定是否允许实例使用主机操作系统中配置好的打印机。如果要使用虚拟打印机，需要为该 ACE 实例添加一个串口，这将会在策略被启用时自动创建；如果禁用该策略，会删除该口串口。
- ④ 在“Administrator Mode（管理员模式）”策略中，如果启用“Enable-administrator mode”并且设置管理员密码，则在使用 VMware ACE 实例的时候，可以通过输入管理员密码，来修改虚拟机的配置，这包括修改虚拟机内存、网卡、硬盘等，启用管理员选项设置。

说明 仅在 VMware ACE 实例的虚拟机没有运行在“全屏”状态时，管理员模式才能生效。如果虚拟机运行在全屏下，即使启用了管理员模式，也由于不能进入设置项去修改虚拟机的设置。

设置完成后，保存设置退出。

(4) 部署虚拟机到 U 盘。

经过测试之后（在 VMware Workstation 界面中单击“Preview in Player”测试虚拟机及其设置的策略），就可以将虚拟机进行打包，然后分发给最终用户使用。在 VMware ACE Workstation 中，可以创建两种“包”，一种是安装到计算机上使用的“非 Pocket 包”，另一种，是安装到 U 盘或活动硬盘上，并且可以直接在 U 盘或活动硬盘上使用的“Pocket 包”。在本节中创建的“包”属于第二种。

在 VMware ACE Workstation 界面中，单击“Create Pocket ACE package”链接，如图 5-62 所示。开始创建用于活动介质的安装包，主要步骤如下。

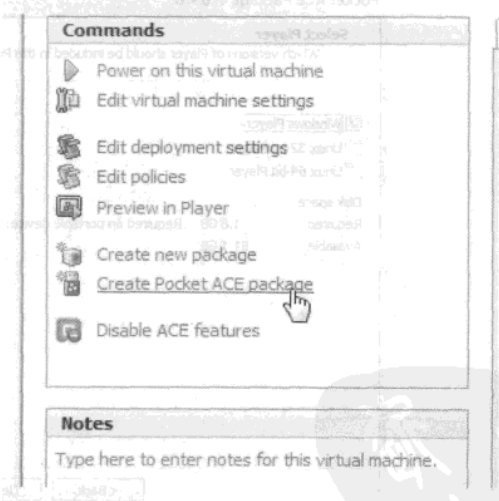


图 5-62 创建用于活动介质的安装包

第 1 步，在“Name the Package”页中，为将要定制的 ACE 实例设置名称“u-xp”，选择保存路径“D:\VM\u-xp\Packages\u-xp”，并且在“Notes”中写上注释信息“package for u pan”，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

如图 5-63 所示。

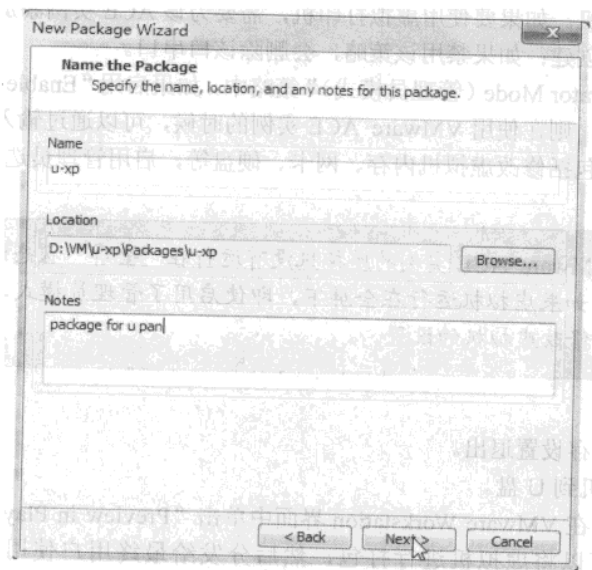


图 5-63 设置“Name the Package”

第 2 步，在“Slecte Player”页中选择“Windows Olayer”复选框，如图 5-64 所示。单击“Next”进入下一页，在“Pocket ACE Deployment Password”页中设置部署口令，本例中密码为 123，如图 5-65 所示，单击“Next”按钮。

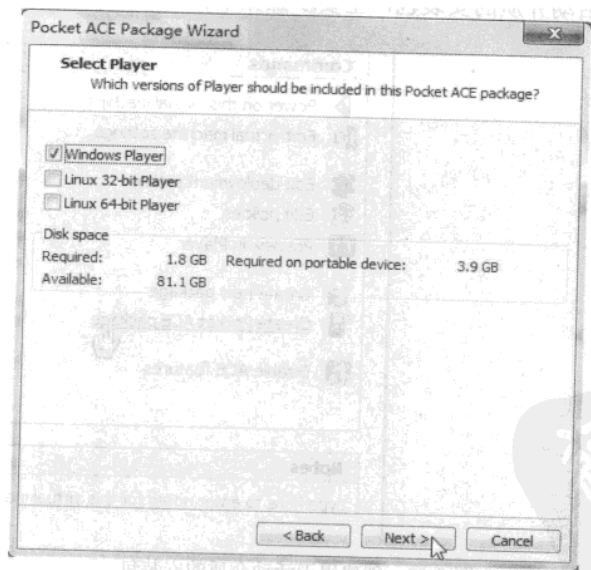


图 5-64 选择“Windows Player”复选框

第 3 步，在“Package Summery”页中核对部署信息，如图 5-66 所示。如果设置信息没有问题，单击“Next”按钮，进入“Completing the Packet ACE Package Wizard”页，如图 5-67

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

所示。选中“Deploy to portable device now”复选框，单击“Finish”按钮，实现立刻向 U 盘（或活动硬盘，或者其他指定位置）部署虚拟机的功能。自动进入“Package Creation”页，开始创建部署虚拟机包，如图 5-68 所示，这个过程大概需要 10 分钟左右。

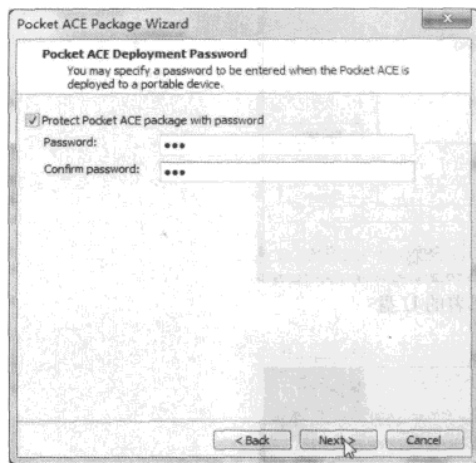


图 5-65 设置部署口令

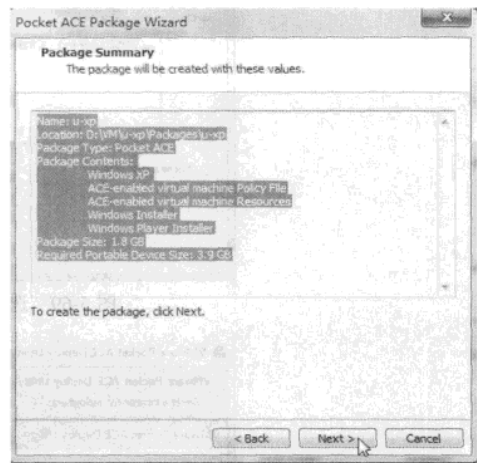


图 5-66 核对部署信息

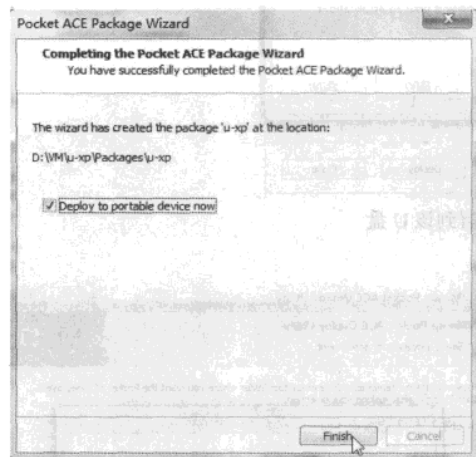


图 5-67 完成设置

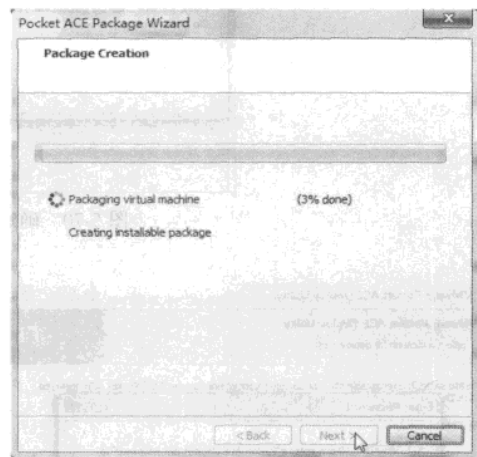


图 5-68 创建部署到 U 盘的包

第 4 步，在“VMware Pocket ACE Deploy Utility”页中，插入 U 盘，单击“Refresh”按钮，在“Choose a removable drive”列表框中，显示出 U 盘及其可用空间大小，如图 5-69 所示。单击“Deploy”按钮开始部署，会弹出部署提示对话框，如图 5-70 所示，单击“是”按钮进入下一页。如果在图 5-65 中设置了部署口令，会弹出“Enter Password”对话框，输入图 5-65 中设置的密码，如图 5-71 所示，单击“OK”按钮，开始向 U 盘部署虚拟机，如图 5-72 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

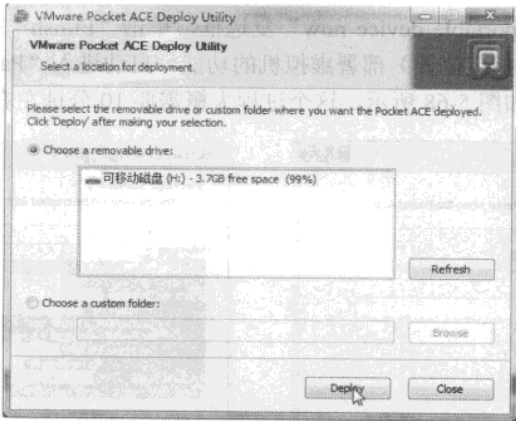


图 5-69 选择要部署的 U 盘

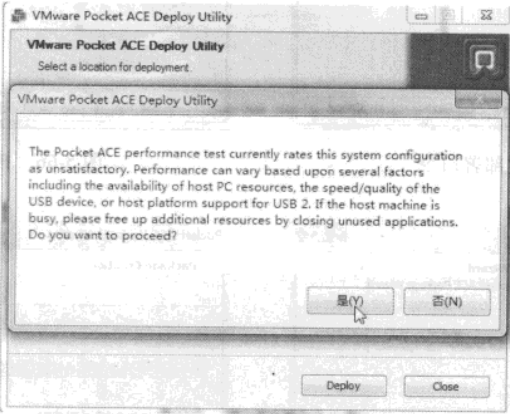


图 5-70 确定要部署到该 U 盘

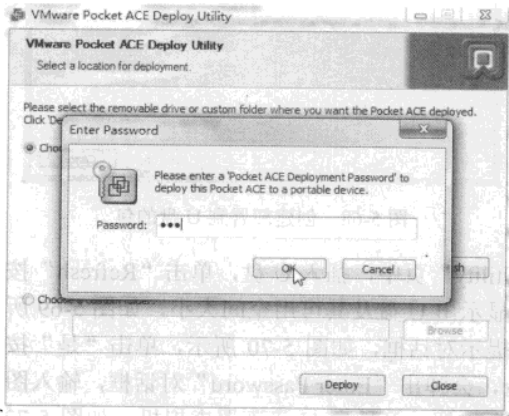


图 5-71 输入部署口令

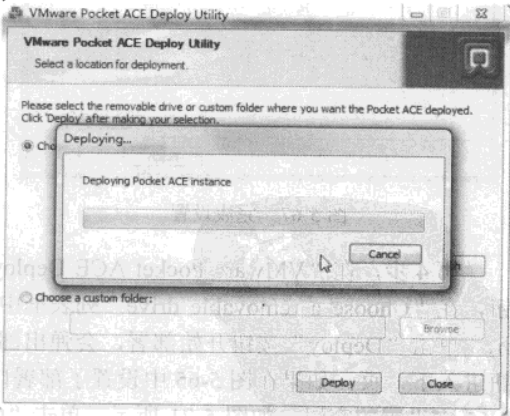


图 5-72 向 U 盘部署虚拟机

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 5 步，部署完成后单击“确定”按钮，然后单击“Close”按钮，如图 5-73 所示。

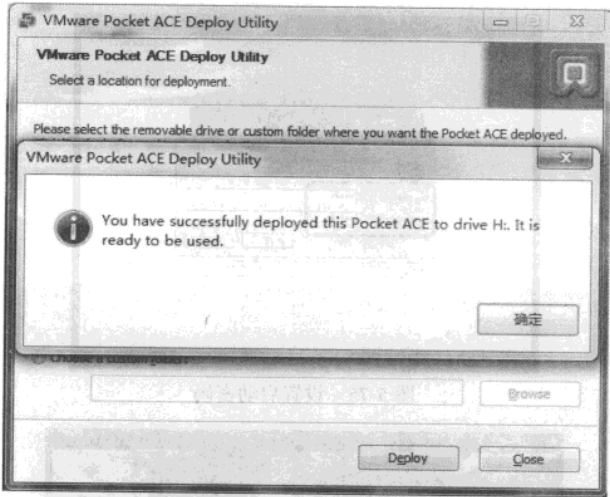


图 5-73 完成部署

(5) 在 U 盘上使用虚拟机。

将 ACE 实例部署到 U 盘后，将 U 盘插入其他计算机，运行 U 盘根目录下的“run.exe”，如图 5-74 所示。将启动虚拟机，如果是第一次使用，将会自动安装 VMware Player，并在安装完成后，进入虚拟机。在虚拟机第一次启动时，需要为虚拟机设置一个密码，如图 5-75 所示。

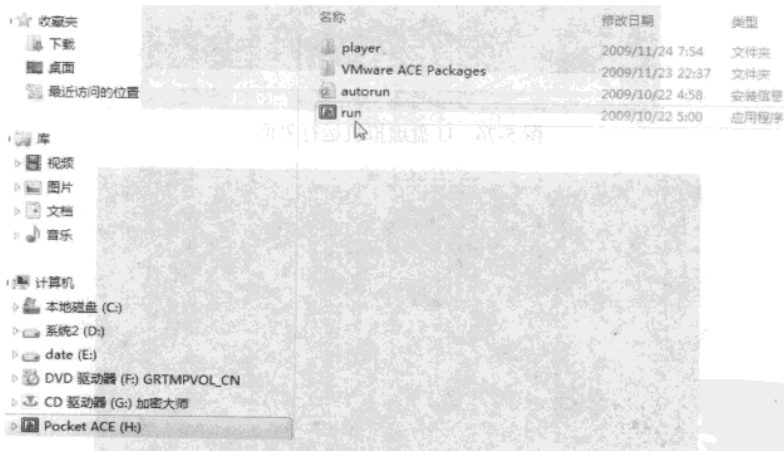


图 5-74 运行“run.exe”

注
意

需要记住该密码，以后每次使用该虚拟机，都要输入这个密码。如果你忘记了密码，需要从管理员处获得恢复密码才能继续使用虚拟机。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

从 U 盘启动虚拟机后的界面如图 5-76 所示。退出的方法是正常关机即可退出，如图 5-77 所示为关机界面。

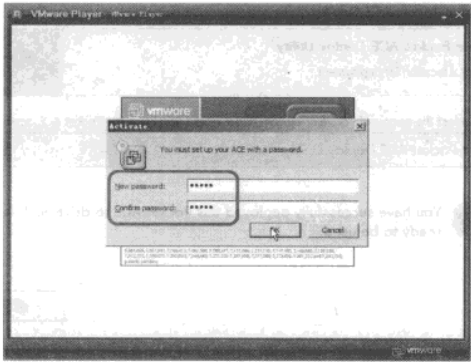


图 5-75 设置启动密码



图 5-76 U 盘虚拟机运行界面

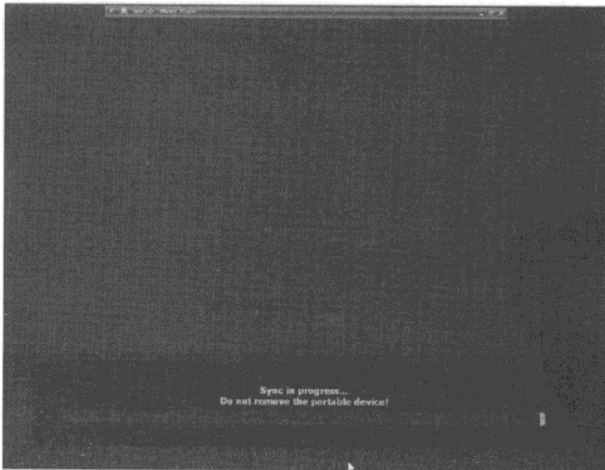


图 5-77 U 盘系统关机界面

说明：VMware ACE Player 需要 License 才能使用，如果将 VMware ACE Player 用于商业环境，你需要从 VMware 公司购买相关的 License。如果要在从没有安装过虚拟机的主机上运行该 U 盘虚拟机，且只是用于测试，可以在部署 VMware ACE 虚拟机后，用“记事本”编辑一个扩展名为 cmd 或 bat 的文本文件，内容如下：

```
echo 正在添加注册表项目...
set regadd=reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup
%regadd% /v "SourcePath" /d "%systemroot%\inf" /f
set regadd=reg add "HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.
%regadd% /v Core /d "VMware Workstation" /f
set regadd=%regadd%\VMware Workstation
%regadd% /v "InstallPath" /d "%cd%" /f
set regadd=%regadd%\License.ws.6.0.200907
%regadd% /v "StartFields" /d "Cpt, ProductID, LicenseVersion, LicenseType,
Epoch" /f
%regadd% /v "Cpt" /d "COPYRIGHT (c) VMware, Inc. 1999-2007" /f
%regadd% /v "ProductID" /d "VMware Workstation for Win32" /f
%regadd% /v "LicenseVersion" /d "6.0" /f
%regadd% /v "LicenseType" /d "User" /f
%regadd% /v "Epoch" /d "2009-7-1" /f
%regadd% /v "Hash" /d "6b3d34d9-b34f898e-2600b82e-9f65a272-44f2afe8" /f
%regadd% /v "Serial" /d "X2MUN-MUUD5-T4K9T-44EMK" /f
%regadd% /v "Name" /d "roebin" /f
%regadd% /v "CompanyName" /d "Home" /f
```

然后保存为 ace.cmd 文件，用鼠标双击该文件，即可以使用 VMware ACE Player。

5.2 VM 虚拟机的使用经验

VM 虚拟机相信大多网管员都会用，在这里就不用做过多介绍了。本节分别介绍一下虚拟机网卡出现问题的解决经验，虚拟机中测试 U 盘量产的小经验，以及如何实现 VMware 与主机同步开关机的经验。

5.2.1 关于 VM 虚拟机虚拟网卡问题的小结

VM 虚拟机是虚拟产品中做的最好的，所以网管员大都习惯使用 VM。不知在使用时有没有遇到过什么问题，在这里我把自己在使用过程中遇到的一些问题跟读者分享一下。本节就介绍虚拟机使用中的虚拟网卡相关的问题：包括虚拟网卡不能使用、虚拟网卡功能属性、修改网卡 MAC 地址、新添加的虚拟网卡不能使用等问题。

(1) NAT 网卡变成 VMnet1 的解决。

问题 1：在 VMware 的所有产品中（包括 VMware Workstation、VMware Server、VMware GSX Server 等），NAT 默认网卡是 VMnet8。但在某些计算机上，NAT 的网卡显示使用的是 VMnet1，如图 5-78 所示。

解决方法：经过仔细查看发现出现这种情况的原因是用户修改了“NAT”选项卡中的虚

网管天下 网管经验谈

拟网卡，虽然这种情况下不影响虚拟机的使用，但许多用户不习惯。此时，可以在图 5-78 所示中，打开“NAT”选项卡，在“VMnet host”下拉列表框中选择“VMnet8”，然后单击“确定”按钮即可，如图 5-79 所示。

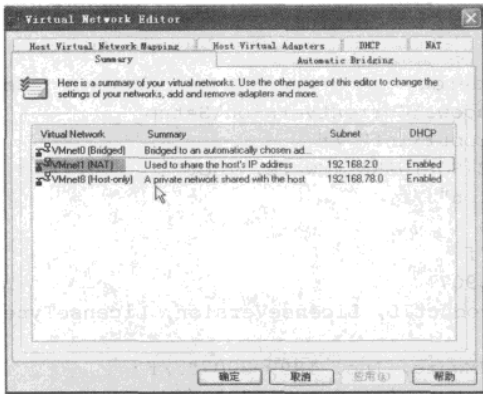


图 5-78 VMnet1 网卡的属性是 NAT

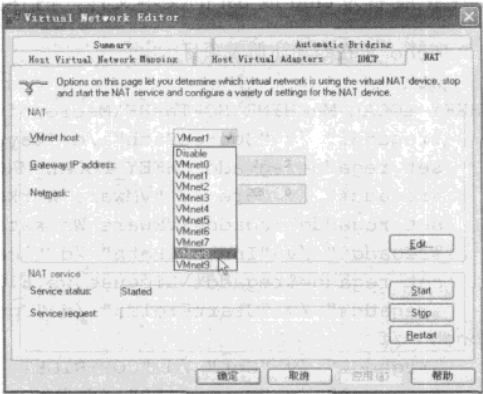


图 5-79 为 NAT 选择虚拟网卡

(2) VMnet8 (NAT) 或 VMnet1 (Host-Only) 网卡变灰的解决方法。

问题 2：在使用 VMware Workstation（或 VMware GSX Server、VMware Server 等产品）创建虚拟机时，发现 VMnet1（或 VMnet8）虚拟网卡选项“变灰”不能使用，如图 5-80 所示。

解决方法：

① 进入“Virtual Network Editor（虚拟网络设置）”界面，在“Host Virtual Adapters（主机虚拟网卡）”选项卡中，单击“Add”按钮，添加 VMnet1（VMnet8）虚拟网卡，如图 5-81 所示。

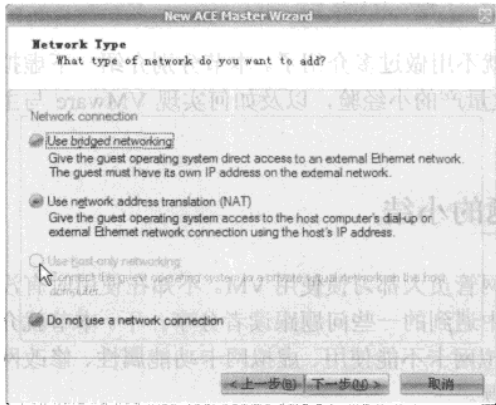


图 5-80 VMnet1 变灰

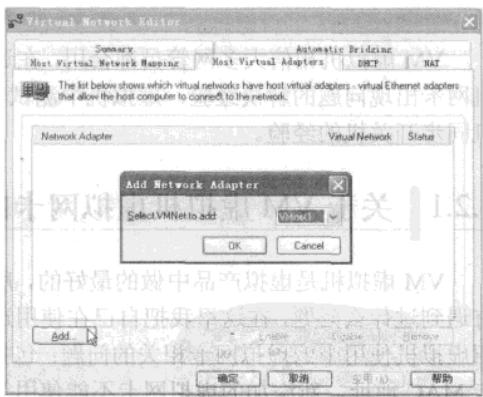


图 5-81 添加 VMnet1 虚拟网卡

② 进入“计算机管理→系统工具→设备管理器”界面，在右侧的“网络适配器”中，查看 VMnet1（或 VMnet8）的状态，如果设备前有红色的“X”号，表示设备被禁用，如果有黄色的“？”号，表示设备驱动程序有问题。如果是前者，启用该设备即可，如图 5-82 所示，如果是后者，更新为正确的驱动程序即可。

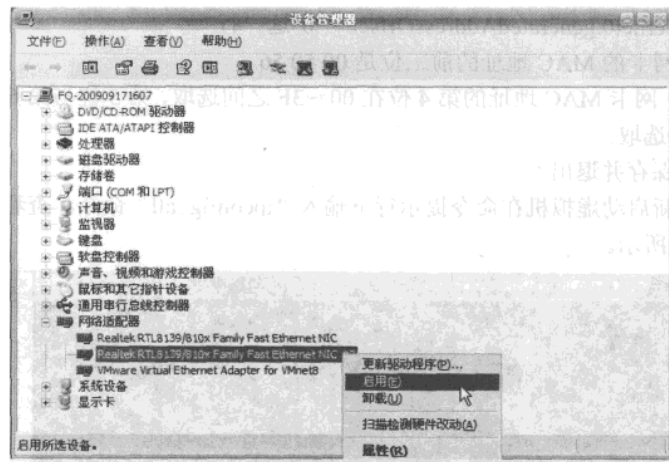


图 5-82 启用被禁用的网卡

(3) 怎样修改网卡 MAC 地址。

有时在使用虚拟机时，需要修改虚拟网卡的 MAC 地址。如果只是需要做普通的修改，可以进入操作系统后用很多种办法做到，但是如果要从根本上修改就没那么容易了（物理网卡需要用编程器重新编写），而在 VMware 虚拟机中，则很容易修改网卡的物理地址。

第 1 步，打开虚拟机目录，找到配置文件，并用“记事本”打开。如果不知道配置文件路径及文件名，可以在 VMware Workstation 主窗口中，打开想要修改网卡 MAC 地址的虚拟机，在“Configuration file（配置文件）”后面可以看到文件路径及文件名，如图 5-83 所示。

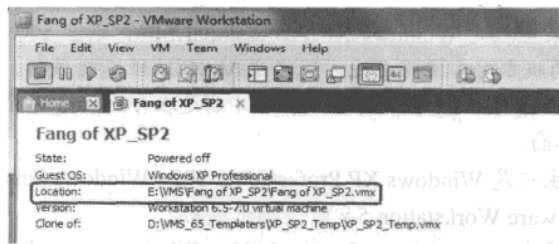


图 5-83 配置文件及保存路径

第 2 步，在打开的文件中，找到如下 3 行：

```
ethernet0.addressType = "generated"
ethernet0.generatedAddress = "00:0c:29:8d:04:61"
ethernet0.generatedAddressOffset = "0"
修改成相应的配置：
ethernet0.addressType = "static"
ethernet0.address="00:50:56:11:22:33"
```

MAC 地址在如下范围中取一个值 00:50:56:00:00:00--00:50:56:3F:FF:FF，如果要修改多台虚拟机的 MAC 地址，注意不要重复。

在第 2 步的操作中注意：

- ethernet0.generatedAddress 是修改为 ethernet0.addressType

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

- 删除 ethernet0.generatedAddressOffset = "0"这一行
- 修改后网卡的 MAC 地址的前三位是 00 50 56
- 修改后，网卡 MAC 地址的第 4 位在 00~3F 之间选取，第 5 位与第 6 位可以在 00~FF 之间选取。

修改完成后保存并退出。

第 3 步，重新启动虚拟机在命令提示行下输入“ipconfig /all”命令，查看 MAC 地址已经更改，如图 5-84 所示。



图 5-84 验证更改结果

注·意

- ① 如果主机是 Windows XP Professional SP3，则在 VMware Workstation 6.0~6.04 的版本时，按照上述方法修改 MAC 地址不能成功。但使用 VMware Workstation 6.5 Beta 版可以成功。图 5-84 则是在 VMware Workstation Beta2 测试成功的界面。
- ② 在主机是 Windows XP Professional SP2、Windows Server 2003、虚拟机版本是 VMware Workstation 5.x 时，测试成功。
- ③ 在主机是 Windows Server 2003、Windows Server 2008、虚拟机是 VMware Workstation 6.5 Beta 时，测试成功。

5.2.2 在虚拟机中测试 U 盘量产的小经验

现在 U 盘量产比较流行，作者也参照制作了一下，比较顺利，但在后期测试 USB CDROM 启动时，出了一些问题，本节就把这些经验跟读者分享一下。

注·意

在进行下面的操作之前，先备份你 U 盘上的数据到本地硬盘，在量产的过程中，U 盘将被初始化。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

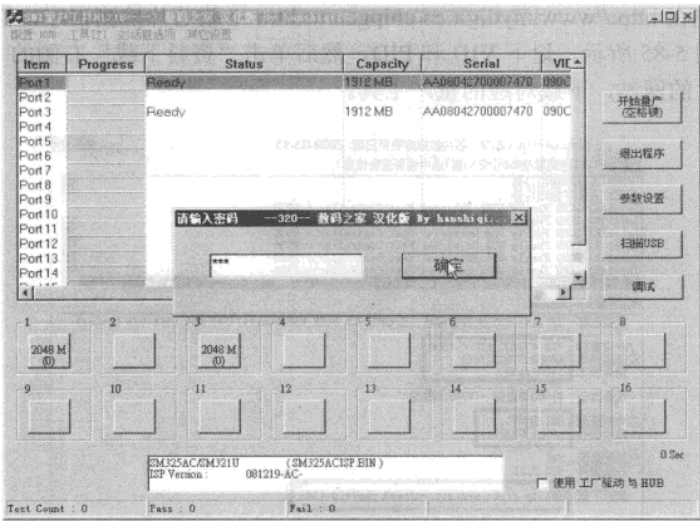


图 5-87 参数设置

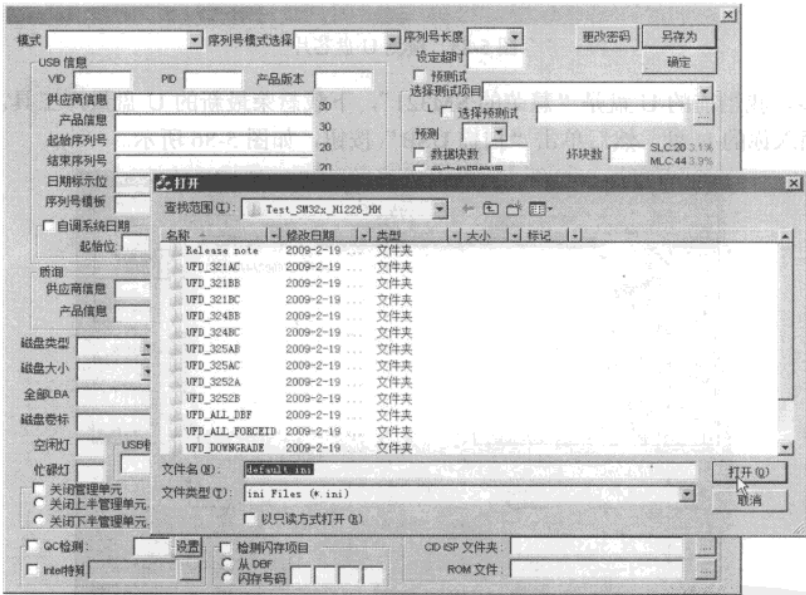


图 5-88 加载配置文件

第 5 步，检查“VID”与“PID”文本框中的数值，与图 5-85 所示中记录的是否一致，如果不一致，请修改为图 5-85 读取的数值。然后选中“制作 CDROM”复选框，单击后面的“”按钮，浏览选择要制作的 CDROM 的 ISO 镜像文件，单击“确定”按钮返回，如图 5-89 所示。

第 6 步，返回到量产工具界面后，单击“开始量产”按钮，如图 5-90 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

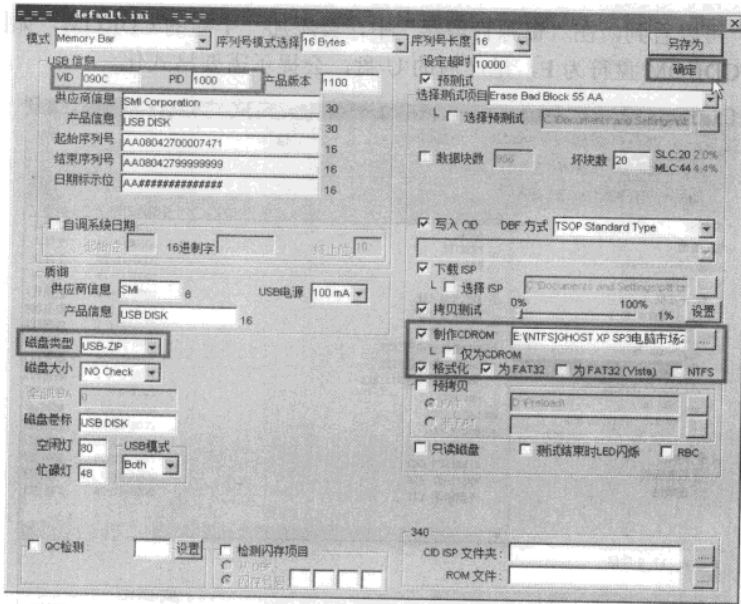


图 5-89 参数设置

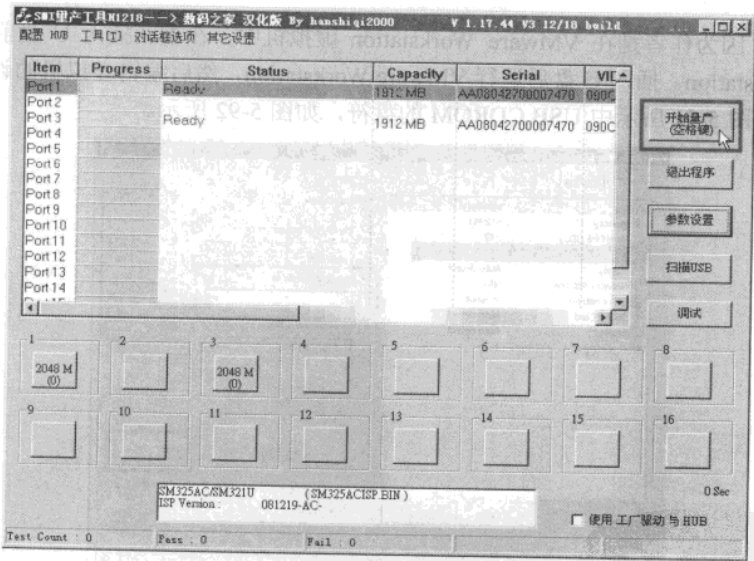


图 5-90 开始量产

说
明

使用该工具可以同时量产多个同一类型、大小的 U 盘。你只需要在 USB 端口中插入想要量产的 U 盘即可。

第 7 步，量产完成后，会弹出“OK”的提示。单击“退出程序”按钮，然后拔出 U 盘，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

接着再次插入，可以看到，在“资源管理器”中，会添加一个新的 CDROM，如图 5-91 所示。
本示例中 USB CDROM 盘符为 F，量产后的 U 盘，会提示需要格式化。

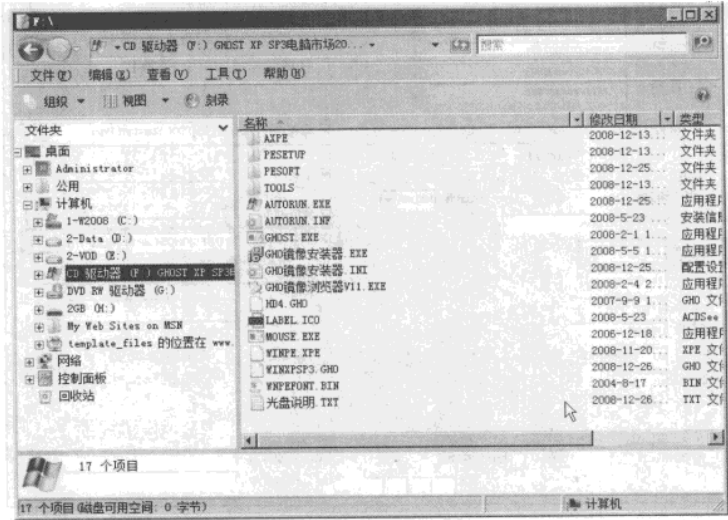


图 5-91 制作成的 USB CDROM

第 8 步，因为作者是在 VMware Workstation 虚拟机中，在重新插入 U 盘前，需要退出 VMware Workstation。插入 U 盘后运行 VMware Workstation，然后编辑虚拟机的设置，让虚拟机的光驱使用图 5-91 所示中 USB CDROM 的盘符，如图 5-92 所示。

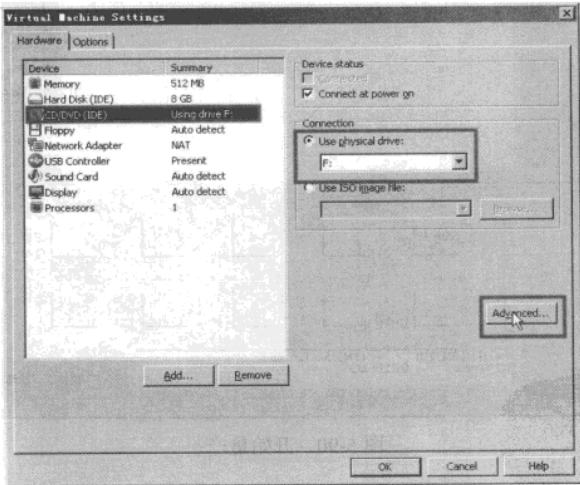


图 5-92 选择 USB CDROM 盘符

单击“Advanced”按钮，选中“Legacy emulation”复选框，单击“OK”按钮，如图 5-93 所示。

第 9 步，启动虚拟机，并进入 CMOS 设置光驱最先引导，就可以看到用 USB CDROM 光盘来启动虚拟机了，如图 5-94 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

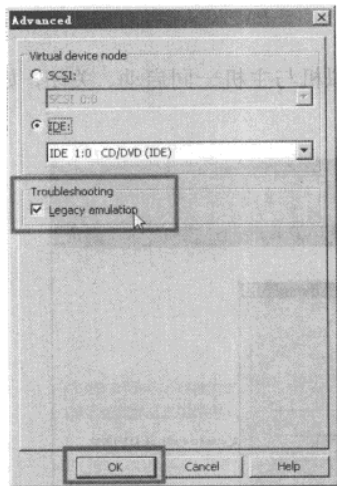


图 5-93 光驱兼容性



图 5-94 用 USB CDROM 启动

经验总结：

- ① 在一开始的时候，作者制作的 USB CDROM，用了多种量产工具，但制作后的 USB CDROM，总是不能在 VMware Workstation 虚拟机中启动，总以为是制作方法的问题，但一直不能启动。
- ② 是不是 VMware Workstation 不支持 USB CDROM？在 VMware 虚拟机设置中，有个光驱兼容性设置的选项在图 5-93 中，设置之后，果然可以使用了。
- ③ 在 Virtual PC 2007 的虚拟机中，发现可以直接使用 USB CDROM 的，界面如图 5-95 所示。



图 5-95 可以在 VPC 2007 中直接使用

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.2.3 轻松实现 VMware 与主机同步开关机

在使用 VMware Server 时，可以设置 VMware Server 的虚拟机与主机一同启动、关闭，如图 5-96 所示。

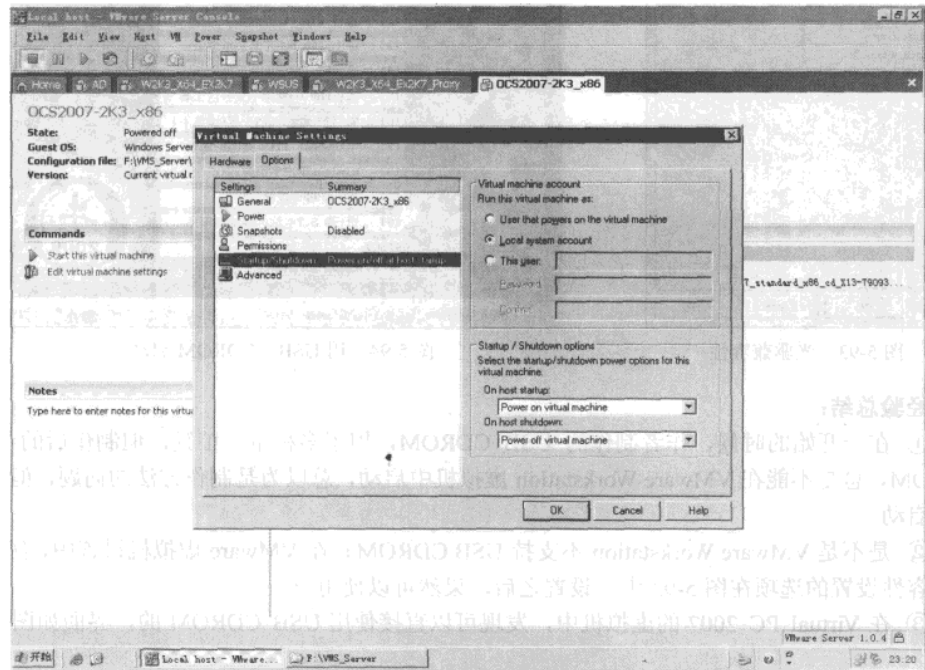


图 5-96 设置虚拟机与主机一同启动、关闭

在实际使用中，当主机启动时（不需要进入登录界面），虚拟机是可以自己启动的。但当主机关闭时，相当于直接单击虚拟机的“关机”按钮，这样虚拟机中的一些服务将不能正常的关闭。虽然 VMware 提供了关机脚本，但脚本中却没有内容，需要我们自己编写。本节就介绍一下如何实现 VMware 与主机同步开关机。

进入虚拟机，进入 VMware Tools 的安装文件夹，在“C:\program files\VMware\VMware Tools”文件夹下，有 4 个批处理程序，分别为：

- poweroff-vm-default.bat，对应于“关机”脚本
- poweron-vm-default.bat，对应于“开机”脚本
- suspend-vm-default.bat，对应于“休眠”脚本
- resume-vm-default.bat，对应于“恢复”脚本

而在“关机”与“休眠”脚本中，并没有对应的“关机”与“休眠”命令，我们需要“手动”加上。具体内容如下：

第 1 步，将这 4 个脚本的“只读”属性去掉，在 poweroff-vm-default.bat 批处理中，添加：“Shutdown /s /t 1”关机命令，意思是 1 秒钟关机。

第2步，在 `suspend-vm-default.bat` 批处理中，添加休眠命令：“`Shutdown /h`”，实现自动休眠功能。

做了以上一点微小的添加后，我们的虚拟机就能实现在主机关机时，虚拟机同步“正常关机”。

在 Microsoft Virtual Server 2005 虚拟机中，当主机关机时，虚拟机可以“休眠”，如果你想实现这样的功能，将 `poweroff-vm-default.bat` 的“关机”命令，改成“休眠”命令就可以了。

5.3 使用 VM 做实验的经验

每一个网管员都有自己做一些网络改造或是增强网络安全的意识，但并不是每一个单位都有实力给网管员提供实验的硬件设备，而又不可能拿单位的计算机做试验否则可能会造成不可预知的损失，所以这就需要 VM 虚拟机的帮助来完成一些网络实验。本节就分别介绍一些用 VM 做试验所遇到的问题及相关经验总结。

5.3.1 VMware License Server 使用经验

在使用 VMware License Server 的时候会碰到一些问题，本节将介绍常遇到的一些问题及解决方法。

（1）复制 License 文件。

在安装 VMware VirtualCenter 的时候，会一同安装 License Server 服务器。如果用户在安装 License Server 的时候，选择了“我要评估 VMware”，在 60 天评估期后，需要购买 License，才能继续使用。那么，怎样导入 License 呢？

如果用户在安装 VMware VirtualCenter 的时候，选择了默认的安装方式，则 VMware License 会安装在 `C:\Program Files\VMware\VMware License Server` 文件夹中，并且评估的 License Server 文件以 `VMware.lic` 的文件名称，保存在“`C:\Program Files\VMware\VMware License Server\Licenses`”文件夹中，如图 5-97 所示。

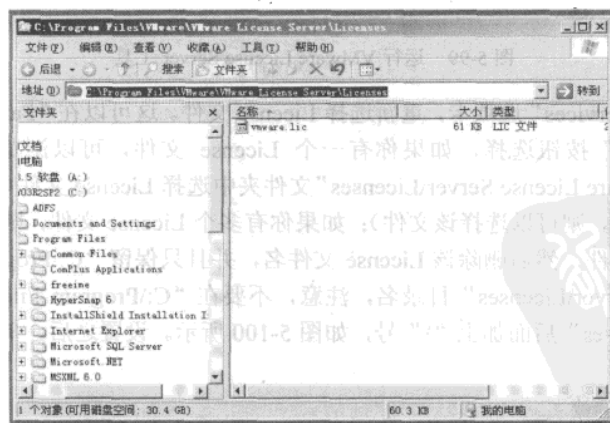


图 5-97 License 文件保存位置

网管天下 网管经验谈

此时，可以将获得的 VMware License 文件复制到“C:\Program Files\VMware\VMware License Server\Licenses”文件夹中，一般情况下，会获得一个 License 文件。在这个 License 文件中，会包括一个 VirtualCenter 与若干个 VMware ESX Server 的许可，也可能会有其他的许可。如果有多个许可文件，也可以将获得的所有许可文件，复制到这个文件夹中。在本例中，作者复制了多个 License 到这个文件夹中，如图 5-98 所示。

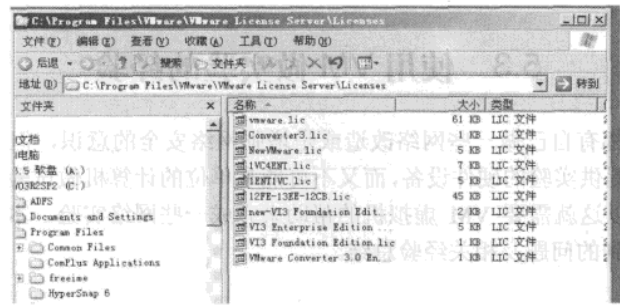


图 5-98 复制了多个许可文件

(2) 重新启动 License Server。
在复制了许可文件后，运行 VMware License Server 工具，如图 5-99 所示。

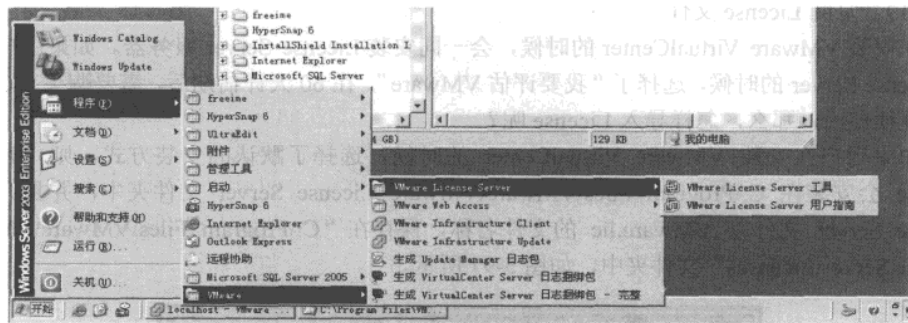


图 5-99 运行 VMware License Server 工具

打开“Config Services”选项卡，重新选择 License 文件。这可以在“Path to the license file”后面单击“Browse”按钮选择，如果你有一个 License 文件，可以浏览并从“C:\Program Files\VMware\VMware License Server\Licenses”文件夹中选择 License 文件（例如，你的 License 文件名为 lvc4ent.lic，则可以选择该文件）；如果你有多个 License 文件，则可以先任意选择其中的一个 License 文件，然后删除该 License 文件名，并且只保留“C:\Program Files\VMware\VMware License Server\Licenses”目录名，注意，不要在“C:\Program Files\VMware\VMware License Server\Licenses”后面加上“\”号，如图 5-100 所示。设置之后，单击右上角的“Save Service”按钮保存。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

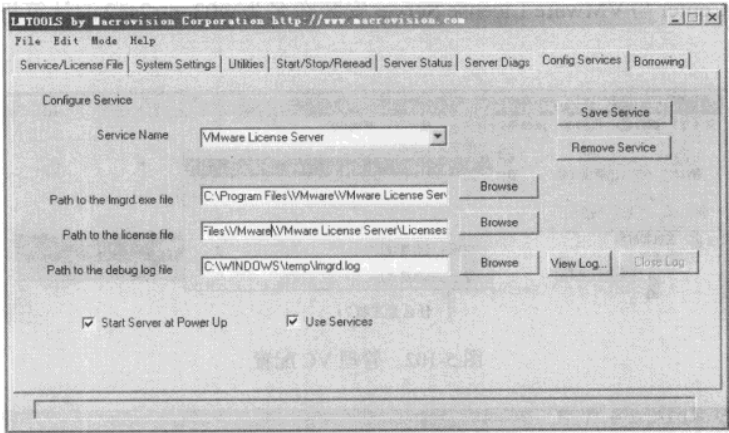


图 5-100 重新指定 License 文件

打开“Start/Stop/Reread”选项卡，依次单击“Stop Server”、“Start Server”和“ReRead License File”按钮，重新加载 License 文件，如图 5-101 所示。

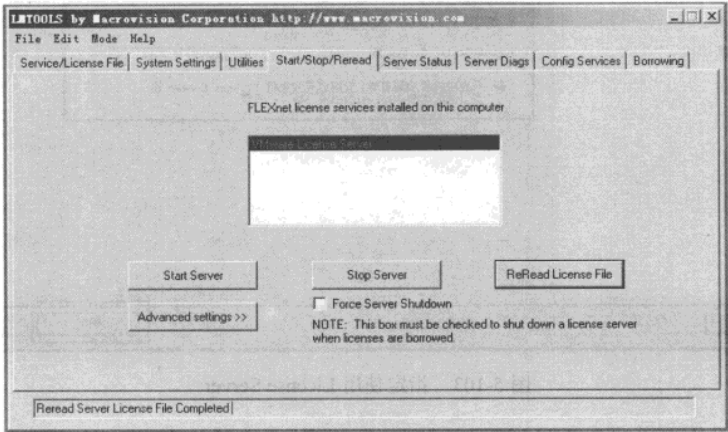


图 5-101 重新加载 License 文件

加载成功后在状态栏会提示“Reread Server License File Completed!”，如果加载失败，说明你在图 5-100 中指定的 License 文件无效，或者在尝试使用多个 License 文件时，输入的路径最后包括了\，即“C:\Program Files\VMware\VMware License Server\Licenses\”。

(3) 配置 VC 使用 License Server。

使用 VI 登录到 VC，从“管理”菜单中选择“VirtualCenter Management Server 配置”选项，如图 5-102 所示。

打开“选择 License Server 设置”界面，在左侧选择“License Server”选项，在右侧取消“评估 VirtualCenter Server”复选框，选中“使用以下 License Server”单选按钮，并且以“端口@计算机名”的格式，输入 License Server 的信息。通常情况下，VMware License Server 使用 TCP 的 27000 端口，而“计算机名”，则是安装 VMware License Server 的计算机名称。在

网管天下 网管经验谈

本例中，VirtualCenter与VMware License Server安装在名为w03entr2sp2的计算机上，如图 5-103 所示。

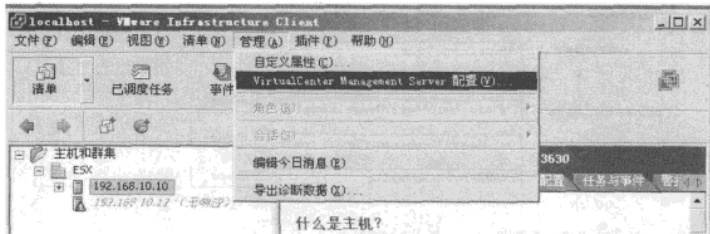


图 5-102 管理 VC 配置

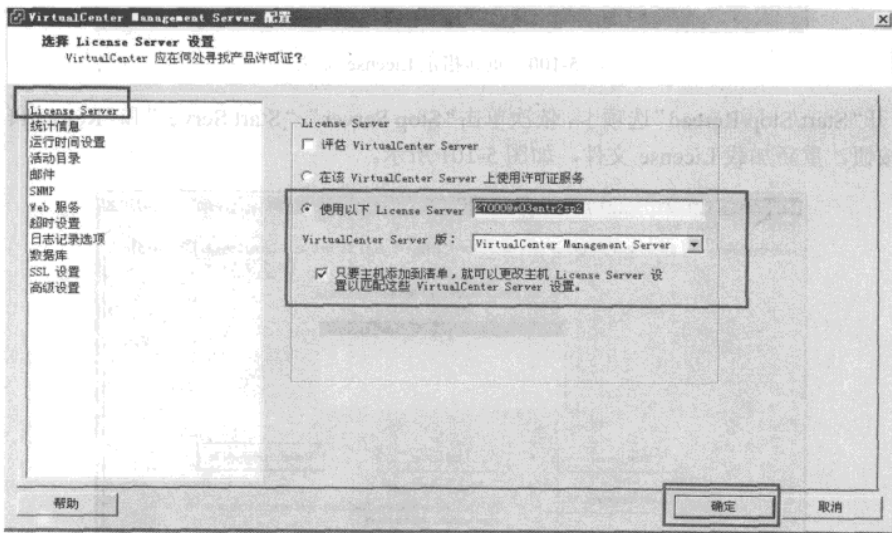


图 5-103 指定使用 License Server

设置之后，单击“确定”按钮，返回到 VI 控制台，单击工具栏上的“管理”按钮，然后打开“许可证”选项卡，可以看到，当前 License Server 已经安装的许可证，如图 5-104 所示。其中，“总计”列表中是已经安装在 VMware License Server 中的许可证，而“剩余”一列显示的是可以使用的许可证的数量。

(4) 配置 ESX Server 使用 License Server 提供的许可证。

设置 VMware ESX Server 使用 License Server 提供的许可。在 VI 中，选中一个 VMware ESX Server 主机，打开“配置”选项卡，选择“已获许可的功能”选项，然后单击“许可证源”后面的“编辑”按钮，如图 5-105 所示。

在“许可证源”对话框中，选择“使用 License Server”单选按钮，并且以“计算机名：端口”的格式，输入 License Server 的计算机名称与服务端口，如果服务端口是 TCP 的 27000（默认端口），则可以忽略端口号。需要注意，如果你的 VMware License Server，使用的是 NetBIOS 名称，而不是 DNS 名称；或者你的 VMware ESX Server，只配置了 IP 地址、网关地

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

址，而没有配置 DNS 服务器地址；或者你虽然配置了 DNS 地址，但配置的 DNS 服务器，不能正确解析你的 VMware License Server 的计算机名称，则在输入 License Server 的地址时，请直接使用 License Server 的 IP 地址。在本例中，License Server 安装在 IP 地址为 192.168.10.129 的计算机上，在此直接使用该地址，如图 5-106 所示。

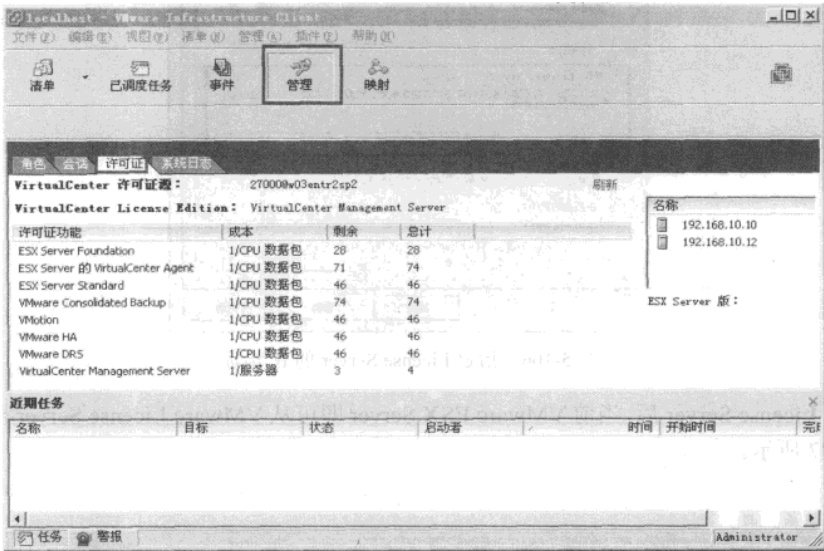


图 5-104 VMware License Server 上已经安装、使用的许可证

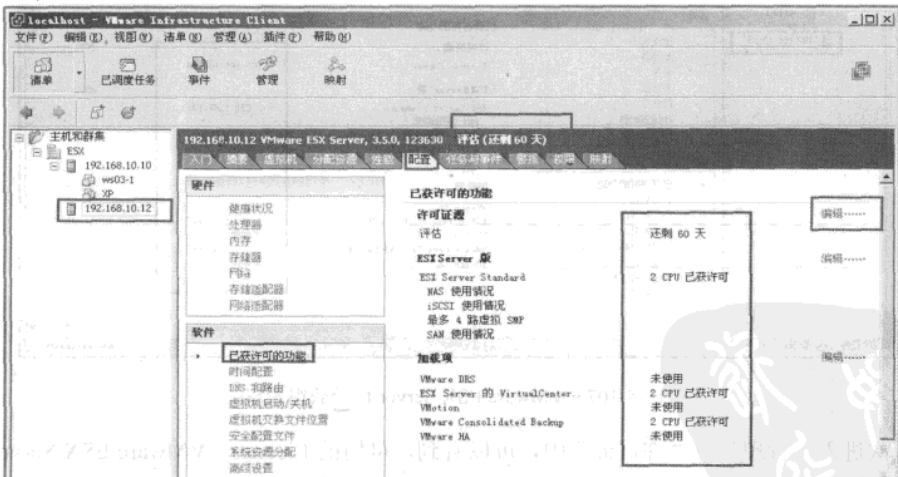


图 5-105 编辑“许可证源”

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

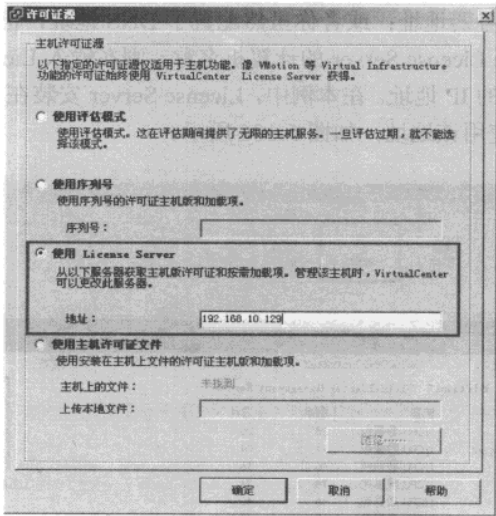


图 5-106 指定 License Server 的 IP 地址

指定 License Server 后,当前 VMware ESX Server 即可从 VMware License Server 获得授权,如图 5-107 所示。

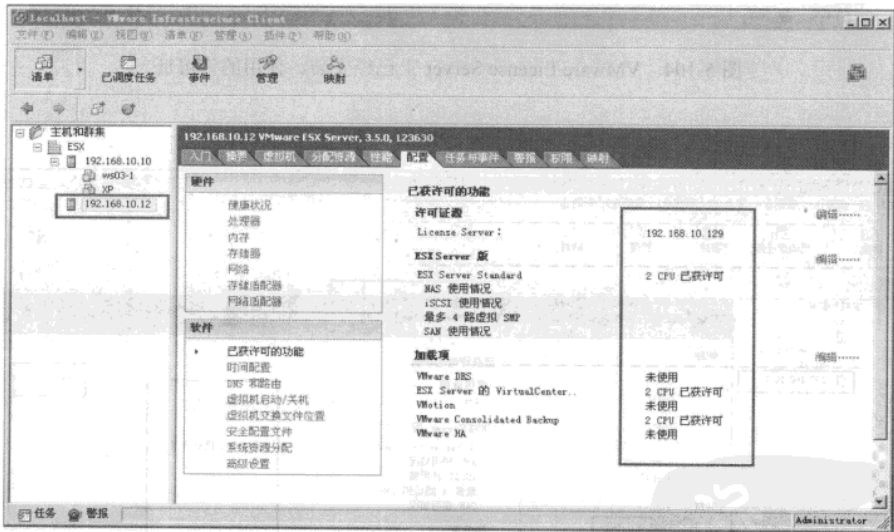


图 5-107 VMware ESX Server 已经获得授权

再次进入“管理”→“许可证”中，可以看到，可用的 License（VMware ESX Server）减少了，如图 5-108 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

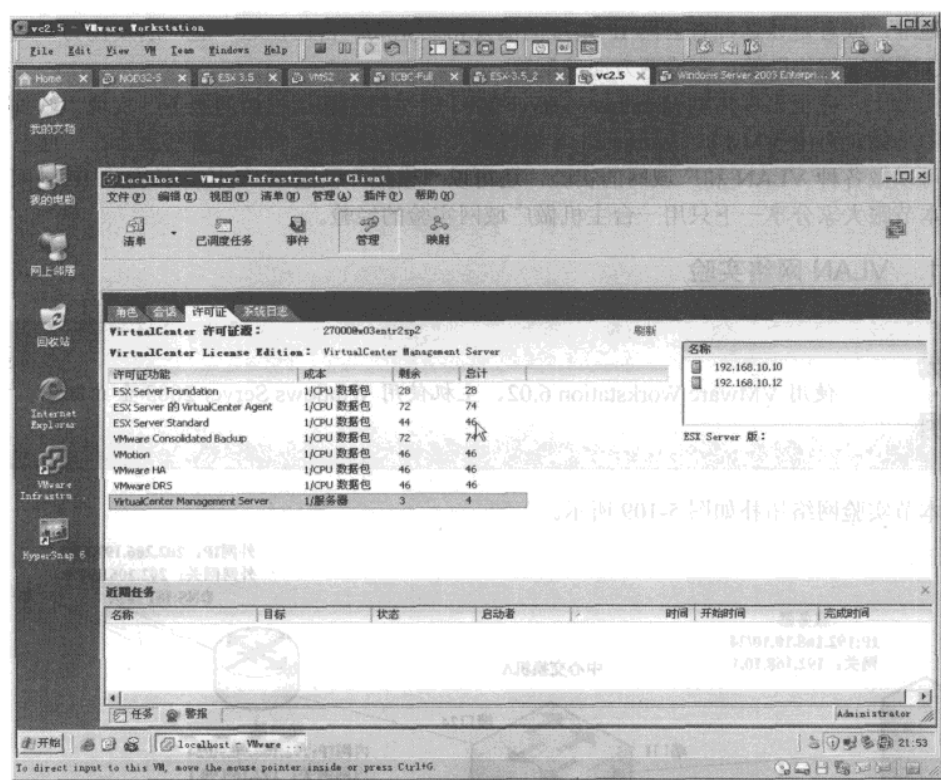


图 5-108 VMware License Server 许可证状况

5.3.2 一台主机实现做广域网实验的方法

很多时候网管员都习惯于用 VMware Workstation 做网络实验，但通常情况下只能做同一个局域网的实验，就是实验中计算机的 IP 地址属于同一个子网。在做广域网与 VLAN 的实验时，通常情况下要借助三层交换机或者路由器才能完成，因为要实现不同网段、不同 IP 之间的“互通”，这只有三层交换机或路由器才能实现。例如：

- (1) DHCP 服务器在为多个 VLAN 分配 TCP/IP 地址、子网掩码、网关地址、DNS 与 WINS 服务器地址时，需要创建多个作用域，并且要在三层交换机支持并要在三层交换机上配置“DHCP 中继”的。如果为了要学习并测试 DHCP 服务器，需要至少一台三层交换机才能完成实现，但不幸的是，许多朋友（尤其是一些学生）是没有三层交换机可用的，还有一些朋友（例如单位网管），手头是没有备用的三层交换机的——单位的三层交换机已经用上了，不可能拆下来做实验。
- (2) 广域网实验，例如 VPN 路由实验，需要至少两个“公网”IP，并且该公网 IP 不在同一个网段上。例如，一个 IP 地址为 61.128.3.65、子网掩码为 255.255.255.248、网关地址为 61.128.3.66，另一个 IP 地址为 202.206.197.100、子网掩码为 255.255.255.128、网关地址为 202.206.197.1。在做这一类实验时，或者是使用两台路由器“背靠背”连接起来并设置为所需

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

要的地址，或者是让远程有公网 IP 地址的朋友帮助完成。自己在这边，朋友在另一边，使用 QQ 或者远程协助等，完成两方面的配置。

实际上，完全可以借助 Windows Server 2003 中“路由和远程访问服务”实现“软件路由器”的功能，再用 VMware Workstation 提供的“虚拟交换机”将两者紧密接合在一起，这样不但可以做各种 VLAN 和广域网的实验，还可以“模拟”任意 IP 地址并且完成 IP 之间的互通。本节跟大家分享一下只用一台主机做广域网实验的经验。

1. VLAN 网络实验

说明

使用 VMware Workstation 6.02、主机使用 Windows Server 2003 企业版。

本节实验网络拓扑如图 5-109 所示。

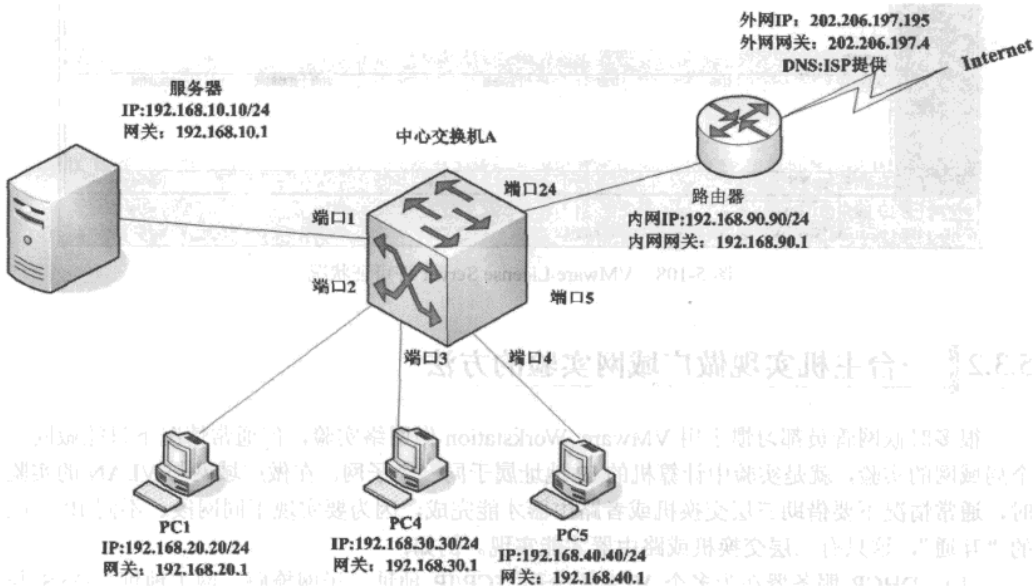


图 5-109 本节实验环境网络拓扑图

在图 5-109 中，划分了 5 个 VLAN（每个端口连接一个不同的子网），对应参数如表 5-1 所示。

表 5-1 VLAN 对应参数

VLAN 名称	所用端口	子 网	端 口 地 址	子 网 掩 码	网络中 PC
VLAN1	端口 1	192.168.10.0	192.168.10.1	255.255.255.0	服务器
VLAN2	端口 2	192.168.20.0	192.168.20.1	255.255.255.0	PC1
VLAN3	端口 3	192.168.30.0	192.168.30.1	255.255.255.0	PC4
VLAN4	端口 4	192.168.40.0	192.168.40.1	255.255.255.0	PC5
VLAN24	端口 24	192.168.90.0	192.168.90.1	255.255.255.0	路由器

其中端口 24 连接路由器，路由器另一端连接 Internet，其他 VLAN 都是通过端口 24 连接的“路由器”访问 Internet 的。

(1) 组建网络环境。

为了实现图 5-110 的环境，需要一台 Windows Server 2003 主机，另外需要两台 Windows Server 2003 虚拟机和 3 台 Windows XP 虚拟机，另外，还需要添加 VMnet2、VMnet3、VMnet4、VMnet5 等虚拟网卡，还要停止主机上的 VMware DHCP 服务。

实验虚拟机网络拓扑如图 5-110 所示。

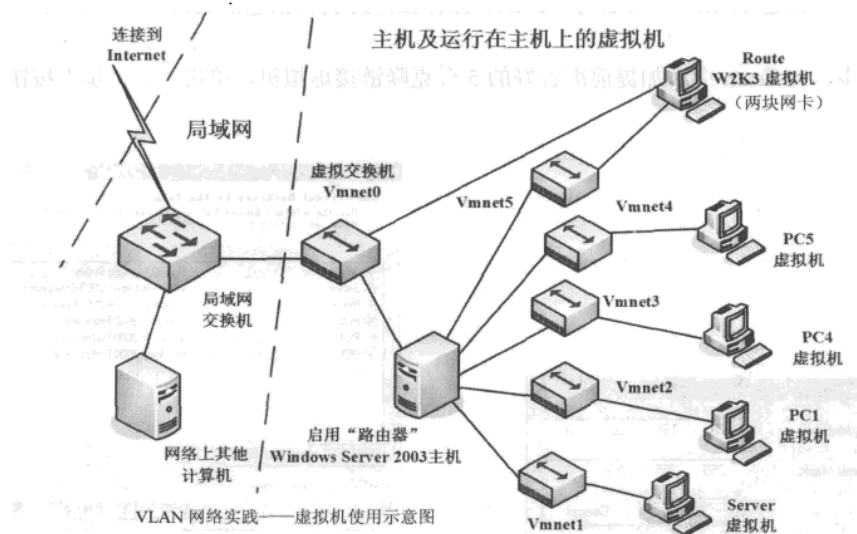


图 5-110 VLAN 实验虚拟机网络连接示意图

实验步骤：

① 主机虚拟网卡设置。

在 Windows Server 2003 主机上，安装 VMware Workstation 6.02，并进行如下的设置。

第 1 步，运行 VMware Workstation，在菜单栏下单击“Edit”按钮，在弹出的菜单中选择“Virtual Network Settings”选项。

第 2 步，在打开的“Virtual Network Editor”页中，选择“Host Virtual Adapters”选项，单击“Add”按钮（这一步是添加虚拟网卡），在弹出的“Add Network Adapter”对话框中，选择“VMnet2”选项，单击“OK”按钮。

第 3 步，按照第 2 步的操作方法，添加 VMnet3、VMnet4、VMnet5 虚拟网卡，添加完成后，单击“应用”按钮，在此需要等待几分钟的时间。

第 4 步，添加网卡完成后，打开“Host Virtual Network Mapping”选项卡。在“Host Virtual Network Mapping”选项卡内，单击 VMnet2 左侧的“>”图标，在弹出的菜单中单击“Subnet”按钮，在弹出的“Subnet”对话框中，设置“IP Address”为“192.168.20.0”，“Subnet Mask”为“255.255.255.0”，然后单击“OK”按钮，如图 5-111 所示。

第 5 步，按照第 4 步方法，设置 VMnet3 网段为 192.168.30.0、VMnet4 网段为 192.168.40.0、VMnet5 网段为 192.168.90.0。

网管天下 网管经验谈

② 创建并编辑 Team。

找一个剩余空间比较大的分区（至少 10 GB 可用空间），例如，在 F 盘 VMX 文件夹下创建 VLAN 文件夹。然后进入 VMware Workstation，创建名为 VLAN 的 Team，并且在 Team 中，添加两台 Windows Server 2003 克隆链接的虚拟机（分别名为 Server 和 Route）、3 台 Windows 2000 Professional 克隆链接的虚拟机（分别名为 PC1、PC4、PC5），如果主机配置比较低，创建 3 台 Windows 98 克隆链接的虚拟机也可。在创建 Team 时，不需要创建 Team 中的 LAN。具体操作步骤如下：

第 1 步，新建 Team，并命名为 VLAN，保存在为此实验创建的文件夹下，单击“下一步”按钮。

第 2 步，向 Team 中添加提前准备好的 5 台克隆链接虚拟机，单击“下一步”按钮，如图 5-112 所示。

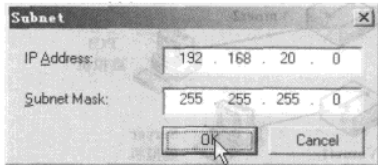


图 5-111 设置 Subnet

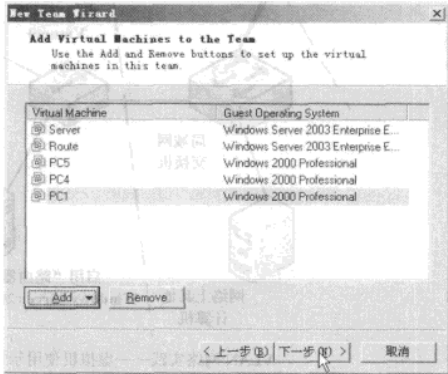


图 5-112 添加克隆虚拟机

第 3 步，在“Add LAN Segments to the Team”对话框中，选择“No, I will add LAN segments later”单选按钮，单击“完成”按钮。

第 4 步，创建 Team 完成后，单击“Edit team settings”链接。

第 5 步，在“Team Settings”对话框中的“Connections”选项卡内，设置 Server 的连接方式为“Host-only”，其余虚拟机为“Bridged”，然后选中“Route”虚拟机，单击“Add Adapter”按钮。

第 6 步，将新添加的网卡的连接方式设置为“Bridged”方式，然后单击“OK”按钮完成设置，如图 5-113 所示。

第 7 步，在 Team 中，选中 Server 虚拟机，用鼠标右击，在弹出的快捷菜单中选择“Settings”命令。在打开的“Virtual Machine Settings”页中，选中声卡，单击“Remove”按钮，将其移除，这样做是为了减轻主机的负担，如果主机配置足够，此步骤可以不做。

第 8 步，在虚拟机设置页中，选中“Floppy（软驱）”选项，并取消“Connect at power on”复选框的选择。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

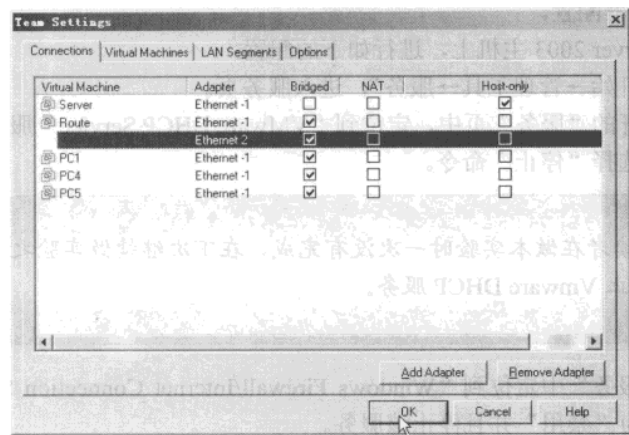


图 5-113 设置新加网卡为桥接方式

第 9 步，在虚拟机设置页的“Hardware”选项卡内，选中“Ethernet”选项，在“Custom”下拉列表框中选择“VMnet1”网卡，单击“OK”按钮，如图 5-114 所示。

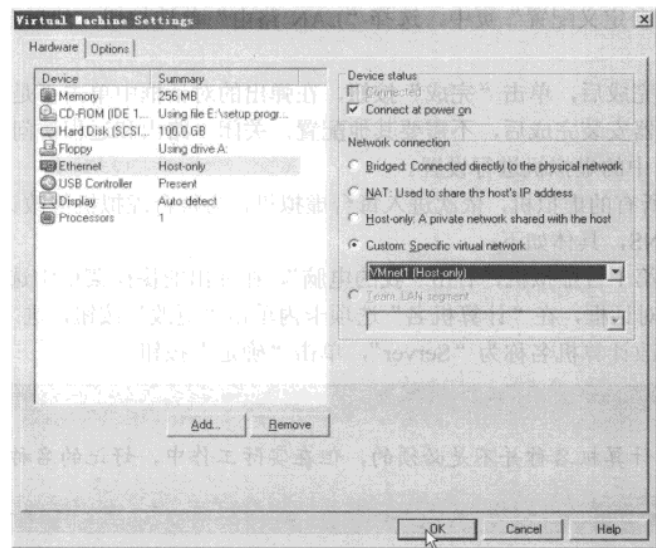


图 5-114 修改虚拟网卡为 VMnet1

第 10 步，同样的方法，编辑 Team 中的每一台虚拟机，删除每台虚拟机的声卡，修改虚拟机的软驱为“不连接”。然后编辑 PC1 使用 VMnet2 网卡、PC4 使用 VMnet3 网卡、PC5 使用 VMnet4 网卡，Route 虚拟机的第 1 块网卡使用 VMnet5，第 2 块网卡使用桥接方式。

说·明 如果没有公网 IP 地址，又想用“合法 IP”地址进行实验，可以通过修改 VMnet8 的“Subnet”的网段地址并且让 Route 虚拟机的第 2 块网卡使用“NAT”的方法做到。

网管天下 网管经验谈

（2）主机路由器配置。

在 Windows Server 2003 主机上，进行如下的配置：

第 1 步，从“开始→管理工具→服务”，进入服务页。

第 2 步，在打开的“服务”页中，定位到“VMware DHCP Service”服务，右击鼠标，在弹出的快捷菜单中选择“停止”命令。

注 · 意

如果读者在做本实验时一次没有完成，在下次继续做实验之前，应该依照图 5-29 停止 VMware DHCP 服务。

第 3 步，从“服务”中定位到“Windows Firewall/Internet Connection Sharing (ICS)”服务，修改启动类型为“禁用”并且停止该服务。

第 4 步，从“管理工具”中运行“路由和远程访问”服务。

第 5 步，在打开的“路由和远程访问”页中，用鼠标右击计算机名，在弹出的快捷菜单中选择“配置并启用路由和远程访问”命令。

第 6 步，在“配置”页中，选择“自定义配置”单选按钮，然后单击“下一步”按钮。

第 7 步，在“自定义配置”页中，选择“LAN 路由”单选按钮，然后单击“下一步”按钮。

第 8 步，配置完成后，单击“完成”按钮，在弹出的对话框中单击“是”按钮。

第 9 步，路由器安装完成后，不需要其他配置，关闭“路由和远程访问”服务。

（3）对 Team 中的虚拟机进行设置。

启动 Team 中所有的虚拟机，依次进入每台虚拟机，为每台虚拟机修改计算机名称、设置 IP 地址及网关、DNS，具体如下：

第 1 步，进入第 1 台虚拟机，右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令，进入“系统属性”对话框，在“计算机名”选项卡内单击“更改”按钮，进入“计算机名称更改”对话框中，修改计算机名称为“Server”，单击“确定”按钮。

说 · 明

修改计算机名称并不是必须的，但在实际工作中，好记的名称易于管理。

第 2 步，修改 IP 地址为 192.168.10.10，网关为 192.168.10.1，如图 5-115 所示。

第 3 步，再进入第 2 台虚拟机，修改计算机名称为“PC1”，设置 IP 地址为 192.168.20.20，网关为 192.168.20.1；进入第 3 台虚拟机，修改计算机名称为 PC4，设置 IP 地址为 192.168.30.30，网关为 192.168.30.1；进入第 4 台虚拟机，修改计算机名称为 PC5，设置 IP 地址为 192.168.40.40，网关为 192.168.40.1。

第 4 步，进入第 5 台虚拟机，修改计算机名称为 route，修改第一块网卡的网络连接名称为 LAN，修改第二块网卡的网络连接名称为 Internet。

第 5 步，设置第 5 台计算机的“LAN”网卡 IP 地址为 192.168.90.90，网关地址为 192.168.90.1。

第 6 步，修改第 5 台计算机的“Internet”网卡 IP 地址为 202.206.197.195，修改网关地址

为 202.206.197.4。

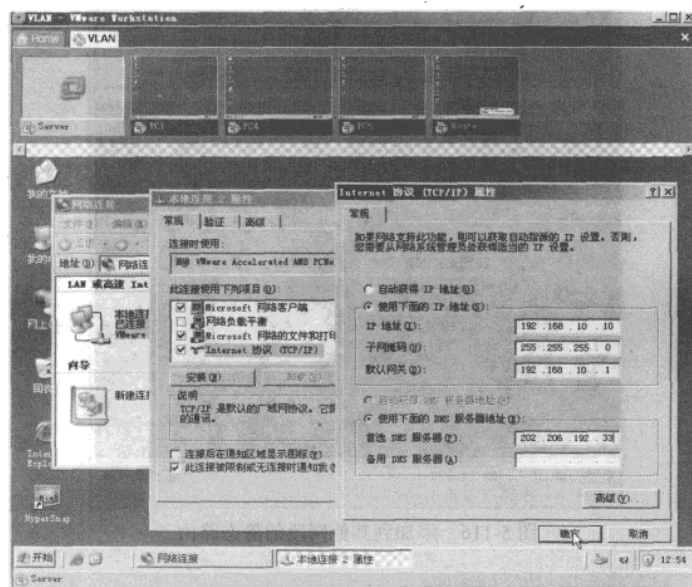


图 5-115 设置第一台计算机 IP 地址及网关、DNS

第 7 步，设置之后，重新启动每台虚拟机，让设置生效。另外，设置 DNS 地址为你的 ISP 提供的 IP 地址，如 202.99.160.68 和 202.206.192.33，这分别是某网通和某大学的 DNS 服务器地址。

第 8 步，在第 5 台虚拟机中，因为没有添加内网网卡的网关，所以其他子网不能访问这台虚拟机。这里可以使用 route 命令，添加到其他子网的路由，命令如下：

```
route -p add 192.168.10.0 mask 255.255.255.0 192.168.90.1
route -p add 192.168.20.0 mask 255.255.255.0 192.168.90.1
route -p add 192.168.30.0 mask 255.255.255.0 192.168.90.1
route -p add 192.168.40.0 mask 255.255.255.0 192.168.90.1
```

其操作如图 5-116 所示。

第 9 步，切换到其他虚拟机中，使用 ping 命令，测试到其他网段，如图 5-117 所示。

(4) 其他实验。

至此各个网段就完成了互通的工作。各 VLAN 之间是可以互相 ping 通的。这就实现了各 VLAN 之间的互通。此后，如果想做 DHCP 服务器的实验，可以在第 1 台虚拟机中安装 DHCP 服务器后为各 VLAN 创建作用域，然后在主机“路由和远程访问”中，添加“DHCP 中继服务”和 DHCP 服务器地址（即名为“Server”虚拟机的 IP 地址 192.168.10.10）即可，有关这些操作的具体步骤不再介绍。

如果要做广域网的实验，将 VMnet2、VMnet3、VMnet4 的地址，换成广域网的地址，并且在虚拟机中根据需要添加相应的地址即可。有的时候还需要在 Team 中添加 LAN1、LAN2 等虚拟网卡，以组成广域网环境进行实验，这些本节也不再介绍。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈



图 5-116 添加到其他网段的静态路由



图 5-117 测试到其他网段的互通

2. 使用 VMware Workstation 虚拟机做网络实验的经验

目前大多数做网管的都没有参与单位已有网络的建设，他们在接手时，都是已经建好的网络。如果这些朋友想学习组网、学习与单位网络相类似的网络组建、服务器与工作站的配置等，只能自己找环境做实验了。虽然单位的设备很全、单位的计算机配置也很高，但为了怕实验过程中把单位的网络“搞坏”，例如，你想做 DHCP 的实验，如果单位的计算机都是从你实验的 DHCP 服务器获得 IP 地址，这些计算机就可能访问不了单位的网络。也有的朋友虽然有

虚拟化应用方面 | 5

独立的网络环境，但苦于不知道做那些实验、从那些实验做起。但是，现在有了虚拟机、有了 VMware Workstation，你可以在一台高配置的计算机上，做绝大多数的实验，不管是单机实验，还是网络实验。

“工欲善其事，必先利其器”，为了能做本节所列出的所有实验，要求你的主机至少有 512 MB 内存、20 GB 可用硬盘空间，推荐 1 GB 或者更高内存、40 GB 可用空间，还要求主机至少有一块网卡，通过单位网络或者通过宽带路由器共享上网，推荐使用 17 in 的 CRT 显示器或者 15 in 液晶显示器，屏幕分辨率至少为 1024×768 以上，不推荐使用宽屏显示器。

（1）基础知识。

在学习虚拟机软件之前，我们需要了解一下相关的一些名词和概念。

主机和主机操作系统：安装 VMware Workstation（或其他虚拟机软件如 Virtual PC）软件的物理计算机称做“主机”，它的操作系统称做“主机操作系统”。

虚拟机：使用 VMware Workstation（或其他虚拟机软件如 Virtual PC，下同）这套软件，由 VMware Workstation “虚拟”出来的一台计算机，这台虚拟的计算机符合 x86 PC 标准，这台计算机也有自己的 CPU、硬盘、光驱、软驱、内存、网卡、声卡等一系列设备，这些设备是由 VMware Workstation 这套软件“虚拟”出来的，但是，在操作系统与应用程序看来，这些“虚拟”出来的设备也是标准的计算机硬件设备，它也会把这些虚拟出来的硬件设备当成真正的硬件来使用的。虚拟机在 VMware Workstation 的窗口中（或全屏状态下）运行，可以在虚拟机中安装操作系统及软件，如 Linux、MS-DOS、Windows、Netware 及 Office、VB、VC 等。

客户机系统：在一台虚拟机内部运动的操作系统称为“客户机操作系统”或者“客户操作系统”。

虚拟机硬盘：由 VMware Workstation（或其他虚拟机）在主机硬盘上创建的一个文件，在虚拟机中“看成”一个标准硬盘来使用。VMware Workstation 还可以使用物理硬盘作为虚拟机的硬盘，但对于初学者来说，不推荐使用主机硬盘作为虚拟机的硬盘。

虚拟机内存：由 VMware Workstation（或其他虚拟机），在主机提供的一段物理内存，把这段物理内存作为虚拟机的内存。

虚拟机配置：配置虚拟机的硬盘（接口、大小）、内存（大小）、是否使用声卡、网卡的连接方式等。

VMware Tools：为了提高虚拟机的性能，由 VMware 公司开发的、在虚拟机系统中安装的一些工具和驱动程序，包括虚拟机的 SVGA 显示驱动程序、鼠标驱动程序、VMware Tools 控制程序等。在 Virtual PC 虚拟机中，与 VMware 的 VMware Tools 类似的工具称做“Microsoft Virtual PC 附加模块”。

虚拟机配置文件：记录 VMware Workstation（或其他虚拟机，如 Microsoft Virtual PC）创建的某一个虚拟机的硬件配置、虚拟机的运行状况等的文本文件，这个文件与虚拟机的硬盘文件等在同一个目录中保存。

开机/关机：运行或关闭虚拟机。

休眠：计算机在关闭前首先将内存中的信息存入硬盘的一种状态。将计算机从休眠中唤醒时，所有打开的应用程序和文档都会恢复到桌面上。VMware 创建的虚拟机也支持这种方式。

网管天下 网管经验谈

（2）VMware Workstation 功能与用途。

- VMware Workstation 分 Linux 和 Windows 版本，分别安装运行在 Linux 操作系统和 Windows 操作系统下。
- VMware Workstation 虚拟机支持 Linux、Windows、DOS、Netware 等大多数的基于 Intel 的 x86 的 PC 机操作系统。
- VMware Workstation 支持主机与虚拟机之间的“拖曳”功能，可以在主机与虚拟机之间交换文件。
- 支持“虚拟网络功能”，可以使用 VMware 自己的网络，从主机、虚拟机之间通过“VMware 虚拟网络”交换数据。
- 快照功能，支持虚拟机系统的即时镜像和还原。
- VMware Workstation 的虚拟机，可以根据需要，模拟成与主机在同一网络、与主机不在同一网络、与主机没有网络关系的计算机。这就是说，VMware Workstation 提供的虚拟机，可以处于主机网络中的任意位置。

■ 3. VMware Workstation 5.0 的功能与特点

（1）**多次快照与恢复：**VMware Workstation 可以根据用户需求，在使用虚拟机的过程中保存多次“快照”并且可以根据需要，恢复到每个“快照”前的状态，就像 Windows XP 中的“即时还原”功能一样，但比即时还原功能要好。因为“快照”保存的是当时的、完整的系统状态，可以随时还原。

（2）**Team：**这是 VMware Workstation 5.0 新增加的功能。使用 VMware Workstation 5.0 的“项目”功能，可以将多台虚拟机组织到一个项目组中一起管理和使用，并且可以对每个虚拟机进行设置和限制其网络带宽。

（3）**克隆：**这是 VMware Workstation 5.0 新增功能。可以将一个虚拟机（从一个虚拟机的“快照”状态）克隆成一个新的虚拟机，或者克隆一个“链接”虚拟机来使用。

（4）**更好的内存和网络支持：**VMware Workstation 5.0 支持内存共享功能，可以在有限的内存下同时运行更多数量的虚拟机。另外，VMware Workstation 5.0 虚拟机内的网卡速度由以前的 10 MB 提升到 1 GB 速度。

（5）**64 位支持：**VMware Workstation 5.0 支持在 AMD 和 Intel 的 64 位主机系统上安装和运行，其支持的虚拟机操作系统仍然为 32 位；而 VMware Workstation 5.5 除了支持在 64 位主机系统上安装和运行外，还同时支持虚拟机运行 32 位或 64 位操作系统。

（6）**录像：**VMware Workstation 5.0 新增功能。在 VMware Workstation 5.0 中，可以将虚拟机的操作和使用情况录制成 AVI 文件，这对于制作教程、演示录像有很大的帮助。

（7）**V2V 支持：**使用 V2V 工具，可以将 Microsoft Virtual PC 或 Microsoft Virtual Server 的虚拟机导入到 VMware 的虚拟机中使用。VMware Workstation 5.5 可以将 Symantec Live State Recovery 制作的镜像转换入虚拟机，也可以直接打开。还可以无缝运行 Microsoft Virtual PC 和 Microsoft Virtual Server 的虚拟机，而在 VMware Workstation 5.5 以前的版本只能在转换格式后使用，这次则是直接提供支持。另外，其增强的命令行界面可以使重复性操作更为简单。

（8）**支持双路虚拟 SMP：**支持两路 Virtual SMP，可以指派一个或两个 CPU 给虚拟机使用。如果使用这项功能，你的主机 CPU 需要是超线程的或者有多个 CPU。

虚拟化应用方面 | 5

（9）**显存大小修改和D3D支持**：VMware Workstation 5.0提供的虚拟机默认显存为16 MB。从VMware Workstation 5.5.1开始，其提供的虚拟机支持修改显卡显存（可以修改为64 MB和128 MB），同时提供了对D3D的支持。

4. VMware Workstation 安装与配置

VMware Workstation 可以安装在 Windows 2000 及其以上的系统中，推荐安装在 Windows XP 或者 Windows Server 2003 中。在有些网络实验中，需要主机系统是 Windows Server 2003，这些在实验中会有专门的提示。

安装 VMware Workstation 5.5.1 的主机要求系统稳定，最好是一台新安装好的 Windows XP Professional，并且打上 SP2 及 Microsoft 最新补丁。作为主机的 Windows XP Professional，推荐只安装必须的软件如五笔、拼音输入法、压缩解压缩程序 WinRAR、Office 等，不推荐在主机上安装无用的软件，如果需要测试，那就在虚拟机中进行，否则用虚拟机就没意义了。

安装 VMware Workstation 后，进行下面的配置。

（1）为虚拟网卡禁用防火墙。在 Windows XP SP2（或 Windows Server 2003 SP1）的主机上安装 VMware Workstation 后，会在主机上安装两块虚拟网卡。为了让虚拟机可以正常地使用这两块网卡，我们需要对 Windows XP（或 Windows Server 2003）的防火墙进行配置，在这两块虚拟网卡上禁用系统内置的防火墙，如果你使用其他防火墙如卡巴斯基防火墙等，也请正确设置，如图 5-118 所示。

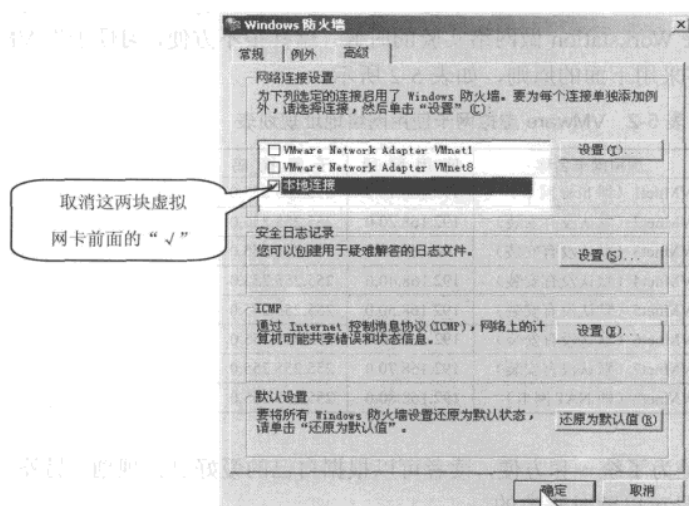


图 5-118 去掉两块虚拟网卡的防火墙设置

（2）设置虚拟机工作目录。在主机上，使用一个剩余空间不小于 10 GB 的分区，在这个分区创建一个新文件夹如 VMS，把这个目录设置为虚拟机的工作目录。

运行 VMware Workstation，从“edit”菜单选择“Preferences”命令，在“Workspace”选项卡中，将默认路径修改为上面创建的 VMS，在本例中为“E:\VMS”，如图 5-119 所示。

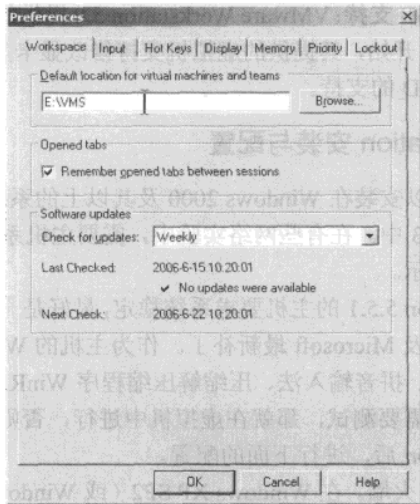


图 5-119 指定虚拟机默认工作目录

(3) 设置虚拟网卡地址范围。默认情况下，VMware Workstation 的虚拟网卡使用 192.168.1.0~192.168.254.0 范围中的（子网掩码为 255.255.255.0）两个网段（对应于第一块虚拟网卡 VMnet1 和第 2 块虚拟网卡 VMnet8），即使在同一台主机上安装 VMware，其使用的网段也不固定。在用 VMware Workstation 做网络实验的时候，这样很不方便，习惯于把 VMware 使用的网段“固定”，通常采用下面的原则，如表 5-2 所示。

表 5-2 VMware 虚拟网卡使用网络地址规划表

虚拟网卡名称	使用网段	子网掩码
VMnet1（即 host 网卡）	192.168.10.0	255.255.255.0
VMnet2（默认没有安装）	192.168.20.0	255.255.255.0
VMnet3（默认没有安装）	192.168.30.0	255.255.255.0
VMnet4（默认没有安装）	192.168.40.0	255.255.255.0
VMnet5（默认没有安装）	192.168.50.0	255.255.255.0
VMnet6（默认没有安装）	192.168.60.0	255.255.255.0
VMnet7（默认没有安装）	192.168.70.0	255.255.255.0
VMnet8（即 NAT 网卡）	192.168.80.0	255.255.255.0

使用表 5-2 的地址只是为了统一和方便，读者可以根据自己的爱好进行规划。另外，在做实验的过程中，这个地址是可以随时修改的。

在“edit”菜单中选择“Virtual Network Settings”命令，在“Host Virtual Network Mapping”选项卡中进行设置，如图 5-120 和图 5-121 所示。

VMnet8 也请修改为 192.168.80.0 网段。其他的 VMnet2 等，由于没有安装相应的虚拟网卡，所以暂时先不要设置，等以后实验需要时，再进行设置。

(4) 虚拟机使用注意事项。

在此不做过多介绍 VMware Workstation 虚拟机软件的使用，为了做好网络实验，推荐你进行下面的准备工作。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

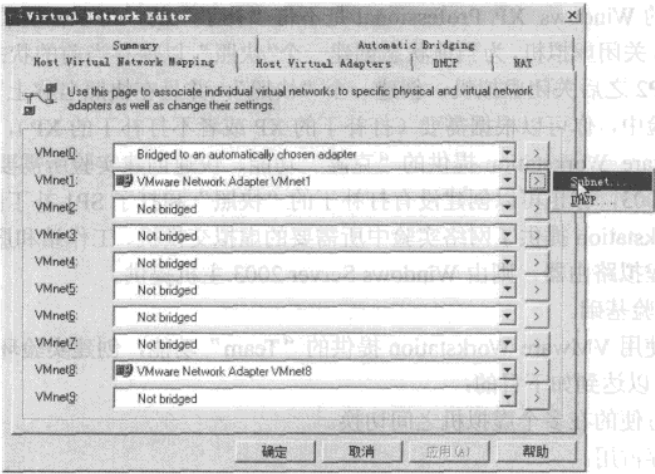


图 5-120 虚拟网卡映射

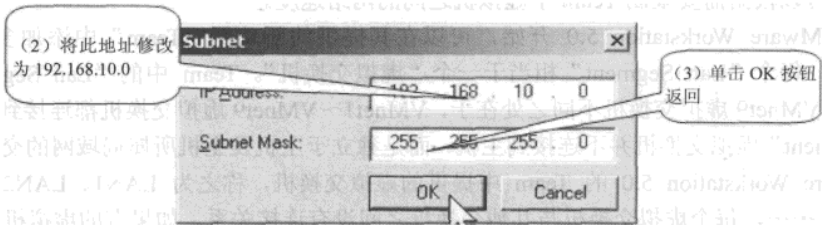


图 5-121 VMnet1 所使用的网段

在一个剩余空间比较大的分区时，使用 VMware Workstation 分别创建 Windows 98、Windows 2000 Professional（带 SP4）、Windows XP Professional、Windows Server 2003 的虚拟机，安装相应操作系统并安装 VMware Tools，如图 5-122 所示。

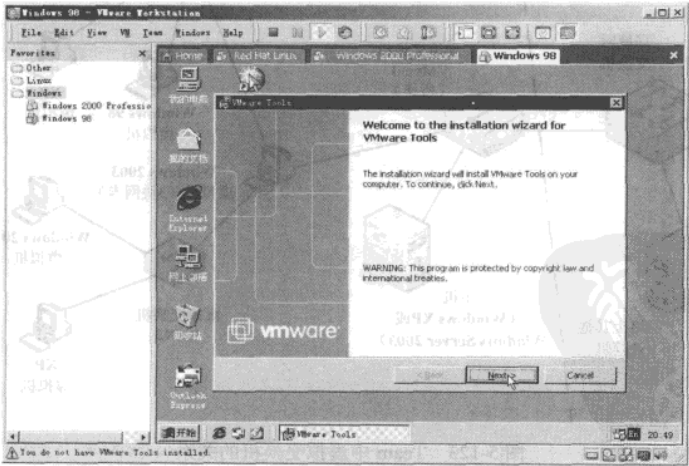


图 5-122 在 Windows 98 虚拟机中安装 VMware Tools

网管天下 网管经验谈

如果你安装的 Windows XP Professional 是不带“补丁”的，可以在安装操作系统并安装 VMware Tools 后，关闭虚拟机，为当前状态创建一个“快照”，以保存当前的状态。安装 Windows XP Professional SP2 之后关闭虚拟机，创建一个“快照”，并且在快照名称上写清相应的信息。这样，在网络实验中，你可以根据需要（打补丁的 XP 或者不打补丁的 XP），从安装好的虚拟机中、使用 VMware Workstation 提供的“克隆”功能、快速创建实验所需要的虚拟机。对于 Windows Server 2003，你也可以创建没有打补丁的“快照”和打了 SP1 补丁的“快照”。

VMware Workstation 提供了网络实验中所需要的虚拟交换机、工作站和服务，对于网络实验中所需要的虚拟路由器，则由 Windows Server 2003 主机提供。

（5）网络实验基础。

下面将介绍使用 VMware Workstation 提供的“Team”功能，创建实验环境的方法。使用“Team”功能，可以达到如下目的：

- 快速、方便的在多个虚拟机之间切换。
- 减少内存占用。
- 可以与主机网络、其他虚拟机网络隔离。
- 可以根据需要限制 Team 中虚拟机之间的网络速度。

从 VMware Workstation 5.0 开始，可以在其提供的新功能“Team”中添加多个“Lan Segment”，每个“Lan Segment”相当于一个“虚拟交换机”。Team 中的“Lan Segment”与 VMnet1~VMnet9 虚拟交换机不同之处在于，VMnet1~VMnet9 虚拟交换机都连接到主机，而“Lan Segment”虚拟交换机并不连接到主机，而是独立于主机及主机所属局域网的交换机。关于 VMware Workstation 5.0 的 Team 中提供的虚拟交换机，称之为 LAN1、LAN2、……、LAN380、……，每个虚拟交换机与其他交换机之间没有连接关系。如果有的虚拟机添加多块网卡，添加多块网卡的虚拟机可以连接多个虚拟交换机，其网络拓扑如图 5-123 所示。

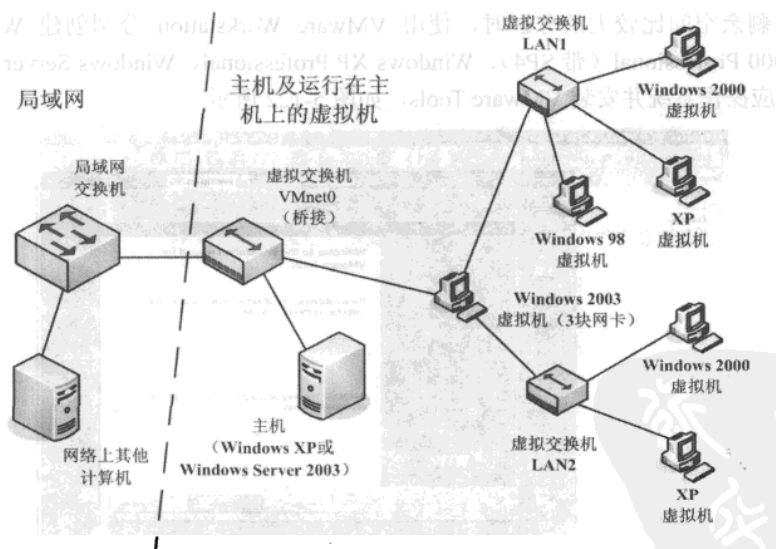


图 5-123 Team 中虚拟交换机的关系

说·明

在图 5-123 中，LAN1 和 LAN2 虚拟交换机并没有直接的网络联系，而是通过一台添加了 3 块网卡的虚拟机联在一起，如果 LAN1 和 LAN2 中的其他计算机（不包括添加 3 块网卡的虚拟机）想要通信，只能通过添加 3 块网卡的 Windows Server 2003 虚拟机（可以通过启用“路由和远程访问”的中“路由器”实现）进行转发。

（6）基本网络实验（DHCP、DNS、WINS）。

实验原因：DHCP、DNS、WINS 服务器是网络中最基本应用，DHCP 服务器用来为网络中众多的计算机自动分配 TCP/IP 地址、子网掩码、网关地址、DNS 服务器地址、WINS 服务器地址等参数；DNS 服务器用来把容易忘记的名称（称做 DNS 名称）解析成对应的 TCP/IP 地址，这样可以减少“寻址”的问题；WINS 服务器用来解析 NetBIOS 的短名称（与 DNS 名称对应，DNS 名称为“长”名称）为对应的 TCP/IP 地址，并且，使用 WINS 服务器，还可以在跨 VLAN 的网络中解决名称解析问题（DNS 服务不存在这个问题）。

本次实验网络拓扑如图 5-124 所示。

实验目的：掌握 DHCP、DNS、WINS 服务器的安装、配置与应用，掌握相关的客户端的配置与使用。

实验引申：根据企业网络的规模，选择是否使用 DHCP、DNS、WINS 服务器，并根据需要进行组合使用。

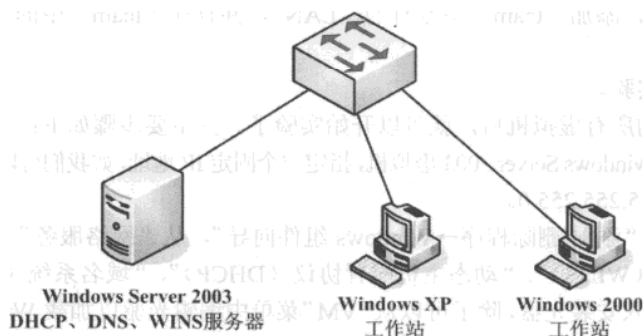


图 5-124 DHCP、DNS、WINS 网络实验拓扑图

实验准备：安装好 Windows Server 2003 操作系统的虚拟机一台，安装好的 Windows 2000 Professional、Windows XP Professional 虚拟机各一台。

本次实验虚拟机拓扑如图 5-125 所示。

5. 使用 Team 功能创建实验环境

在安装好的虚拟机上，为每个虚拟机创建一个“克隆”链接。然后在 VMware Workstation 中创建“Team”，将创建好的“克隆”链接的虚拟机添加到新建的 Team 中，组建实验环境。

① 为了实验和管理方便，在硬盘上为每一个 Team 创建一个文件夹，保存当前实验中的所有“克隆”链接的虚拟机和“Team”，本节将在 E 盘的 VMS 文件夹中创建一个文件夹，文

网管天下 网管经验谈

文件夹名称为“dhcp_dns_wins”。

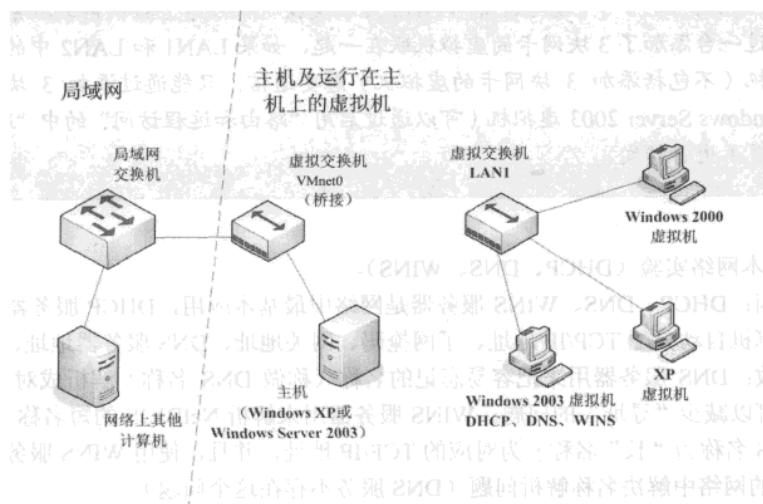


图 5-125 主机、虚拟机组网拓扑图

② 分别在已经安装好的 Windows Server 2003/2000 Professional/ XP Professional 创建“克隆链接”的虚拟机，并将每一个虚拟机保存在上一步创建的文件夹中。

③ 打开 VMware Workstation，新建“team”，创建的过程中添加上一步创建的“克隆”链接的虚拟机。之后，添加“team”中专有的“LAN”，并且让“team”中的虚拟机使用添加的“lan”。

(1) DHCP 实验。

启动 team 中的所有虚拟机后，就可以开始实验了。其主要步骤如下：

第 1 步，进入 Windows Server 2003 虚拟机，指定一个固定 IP 地址，如我们可以使用 192.168.1.1，设置子网掩码为 255.255.255.0。

第 2 步，进入“添加/删除程序→Windows 组件向导”，从“网络服务”中添加“Windows Internet 名称服务 (WINS)”、“动态主机配置协议 (DHCP)”、“域名系统 (DNS)”服务。如果安装程序提示插入安装光盘，除了可以从“VM”菜单中编辑光驱以加载 Windows Server 2003 安装光盘，还可以用鼠标右键单击最小面的状态条，从弹出的菜单中选择“settings”命令，再从弹出的菜单编辑虚拟机的光驱。

第 3 步，从“管理工具”中运行“DHCP”，创建一个作用域，并配置 DHCP 作用域参数。

第 4 步，DHCP 服务器配置完成后，切换到 Windows 2000 虚拟机，进入命令提示符，运行 ipconfig/all 命令，检查是否从 DHCP 服务器获得地址。

(2) DNS 实验。

在本实验中，我们将在 DNS 服务器上创建 DNS 区域（区域名为 heuet.com），并在区域中创建 www 的 A 记录，然后在工作站上解析 www.heuet.com，并验证其正确性，其主要步骤如下。

第 1 步，返回到 Windows Server 2003 虚拟机，进入 DNS 服务器，创建 DNS 区域，区域名称为 heuet.com。

第 2 步，在 DNS 区域中，创建 www 的 A 记录，使其指向服务器 IP 地址，然后进入 Windows

XP 虚拟机，验证其正确性。

（3）共享上网实验。

实验原因：因为 IP 地址有限，以及 Internet 接入费用及使用费用这两个最主要的问题，大多数单位都是“共用”一个到 Internet 的接入，这样就出现了多种共享上网方法。

实验目的：掌握多种软件共享上网的方法，可以根据企业的规模、需求、费用等问题，为企业选择合适的共享上网方法。

实验注意事项：本节实验需要有 Internet 接入，任意一种接入方式都可以。根据 Internet 接入方式的不同，作为服务器的 Windows Server 2003 虚拟机中网卡的连接方式也不相同。

实验准备条件：安装好 Windows Server 2003 操作系统的虚拟机一台，安装好的 Windows 2000 Professional、Windows XP Professional 虚拟机各一台。我们可以继续使用上一节中创建的 team 中的虚拟机。

准备实验环境：使用前一实验中的虚拟机，关闭所有的虚拟机，编辑 team，为 Windows Server 2003 再添加一块网卡，因为共享上网实验需要两块网卡（一块网卡连接局域网，一块网卡连接到 Internet）。

根据用户连接 Internet 的方式不同，新添加的虚拟网卡其属性与设置也不同。如果主机可以直接上网，如有固定的 IP 地址，并且你还有其他的 IP 地址可以使用，则添加的网卡属性可以是“桥接”方式。如果你没有可用的 IP 地址，则添加网卡的属性为“NAT”方式。

如果主机是通过 ADSL 共享上网，并且也想在虚拟机 Windows Server 2003 中通过 ADSL 拨号方式上网，其他虚拟机通过 Windows Server 2003 拨号 ADSL 共享上网，则添加网卡属性为“桥接”方式。如果你不想让 Windows Server 2003 的虚拟机拨号上网，并且使用主机已经拨号上网的 Internet 连接，则虚拟机网卡属性为“NAT”方式。

不管选择哪种方式，我们都可以在以后的实验中，根据需要修改网卡的属性。在这里我们设置网卡属性为 NAT 方式，在 Windows Server 2003 虚拟机中，我们将使用“路由和远程访问服务”中的“NAT”为其他两台虚拟机提供共享上网服务。

在 Windows Server 2003 虚拟机共享上网服务器的配置主要步骤：

第 1 步，启动 team，当所有的虚拟机都启动后，进入 Windows Server 2003 虚拟机，等待一会，系统会自动为新添加的第二块网卡安装驱动程序，并自动把网卡名称命名为“本地连接 2”；原来的网卡名称则为“本地连接”。

第 2 步，打开“网络连接属性”，把原来的网卡（名为“本地连接”）重命名为“LAN”，把新添加的网卡（名为“本地连接 2”）重命名为“Internet”。

第 3 步，设置连接到 Internet 网卡的 IP 地址，因为这块网卡属性是 NAT，设置 IP 地址为 192.168.80.10，子网掩码 255.255.255.0，网关地址设置为 192.168.80.2，设置 DNS 为当地 ISP 提供的 IP 地址。

第 4 步，运行“路由和远程访问”服务，启用 NAT，选择“Internet”为到 Internet 的连接网卡，选择“LAN”为到局域网的连接。

第 5 步，在 Windows 2000、Windows XP 虚拟机中，打开 IE 并进行测试。

5.3.3 在 VMware Workstation 虚拟机中安装 VMware ESX 3I 的经验

在 VMware 网站上，发现 VMware ESX 3I 免费，就第一时间下载了该版本，准备测试一

网管天下

网管经验谈

下。因为手头没有服务器，就在虚拟机中进行测试，主要测试结果如下：

① 可以在 VMware Workstation 中完成 VMware ESX 3I 的安装、虚拟机的创建工作，但不能完成虚拟机的启动。“不能在虚拟机中启动虚拟机”，这是提示信息。

② 不能在 Windows Server 2008 的 Hyper-V 虚拟机中，安装 VMware ESX 3I。

下面介绍在 VMware Workstation 6.5 中安装、测试 VMware ESX 3I 的步骤与过程。

(1) 创建虚拟机并在虚拟机中安装 VMware ESX 3I。

为了在虚拟机中安装 VMware ESX 3I，需要创建“Red Hat Enterprise Linux 3 64-bit”的虚拟机，在创建虚拟机时，按照默认值选择即可。在本例中，为该虚拟机分配 1 GB 内存、设置 80 GB 的虚拟 SCSI 硬盘。创建完虚拟机后，使用 VMware ESX 3I 安装光盘，作为虚拟机的光驱，启动虚拟机，并开始安装，主要步骤如下。

第 1 步，开始安装，如图 5-126 所示，在屏幕的上方显示产品信息、当前计算机（虚拟机）的配置等信息。

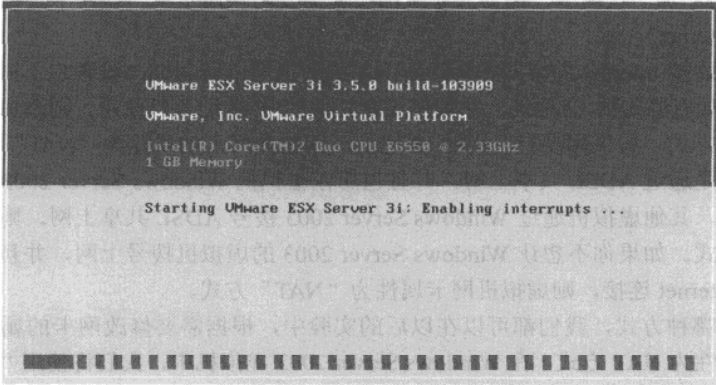


图 5-126 产品信息

第 2 步，显示硬盘信息，选择要安装的硬盘并按 Enter 键继续，如图 5-127 所示。

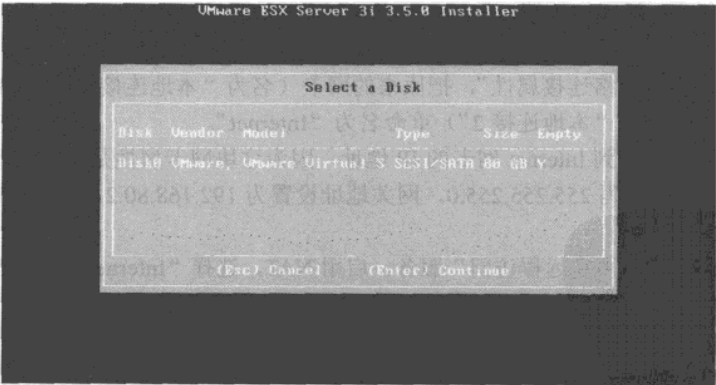


图 5-127 选择安装硬盘

第 3 步，如图 5-128 所示，按 F11 键开始安装。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虚拟化应用方面 | 5

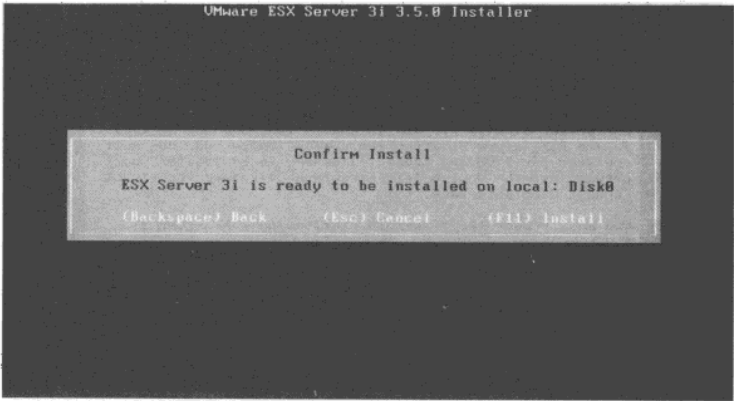


图 5-128 按 F11 开始安装

第 4 步，如图 5-129 所示，按 F11 接受许可协议。

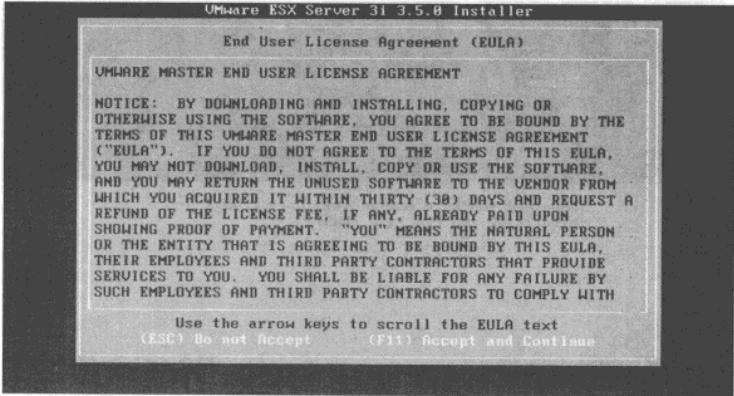


图 5-129 接受许可协议

第 5 步，开始安装，如图 5-130 所示，这一步需要几分钟的时间。

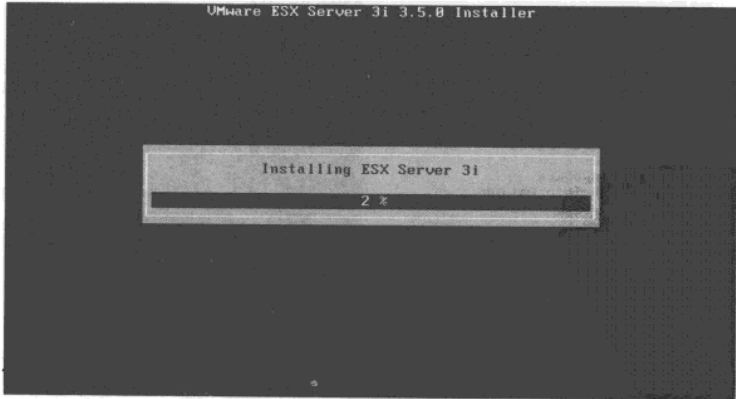


图 5-130 安装界面

第 6 步，安装完成后，如图 5-131 所示，按 Enter 键重启。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

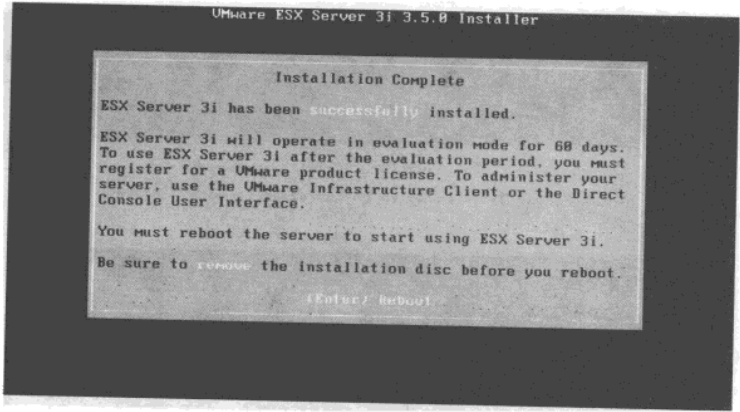


图 5-131 按 Enter 键重启

第 7 步，再次进入系统后，提示管理地址，如图 5-132 所示。

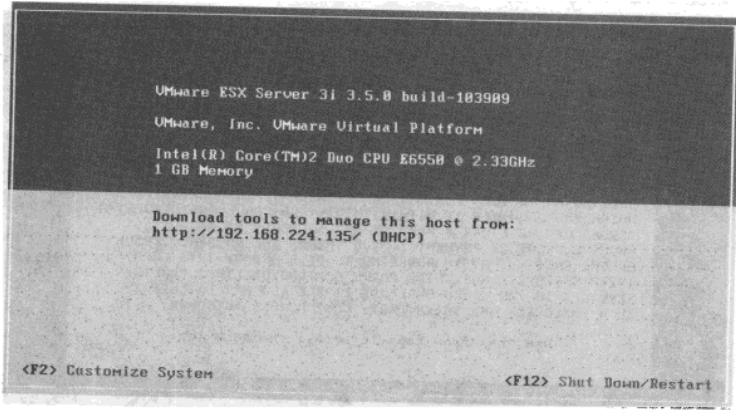


图 5-132 显示管理地址

第 8 步，按 F2 键，进入配置界面如图 5-133 所示。

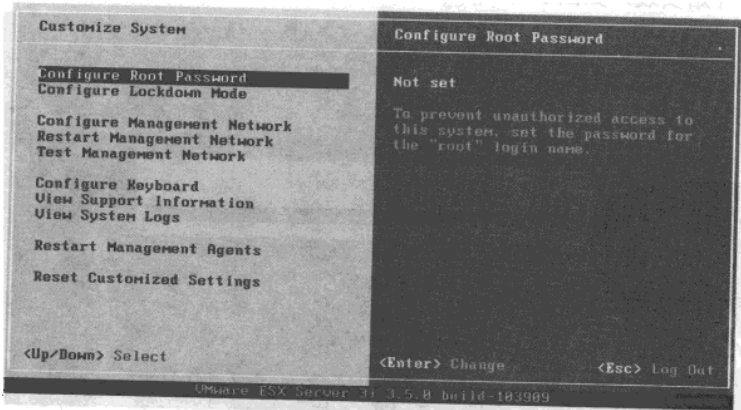


图 5-133 系统定制页

在图 5-133 中，可以设置 root 用户口令，如图 5-134 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

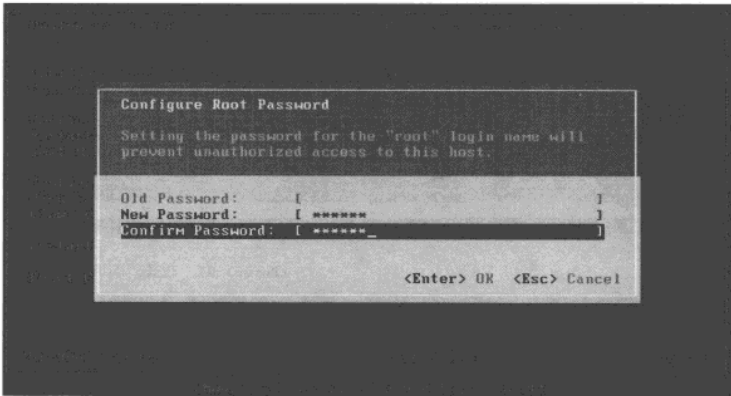


图 5-134 设置 Root 用户口令

第 9 步，在“Configure Management Network”中可以设置主机名称、IP 地址等，如图 5-135 所示。

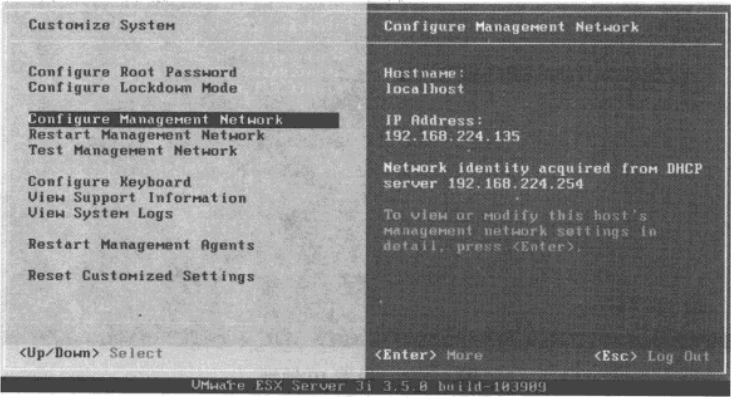


图 5-135 设置主机名称等

在其子菜单中，可以查看网卡 MAC 地址、设置 VLAN、IP 地址等，如图 5-136、图 5-137、图 5-138 和图 5-139 所示。

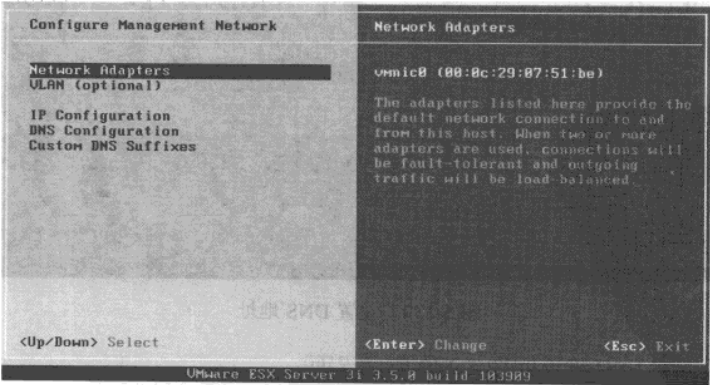


图 5-136 查看 MAC 地址

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

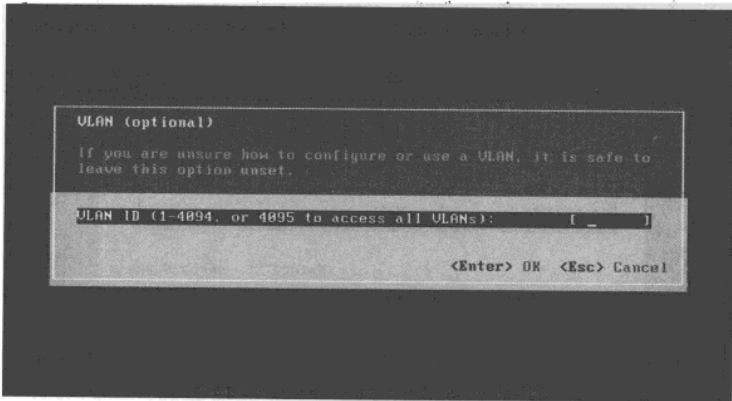


图 5-137 设置 VLAN

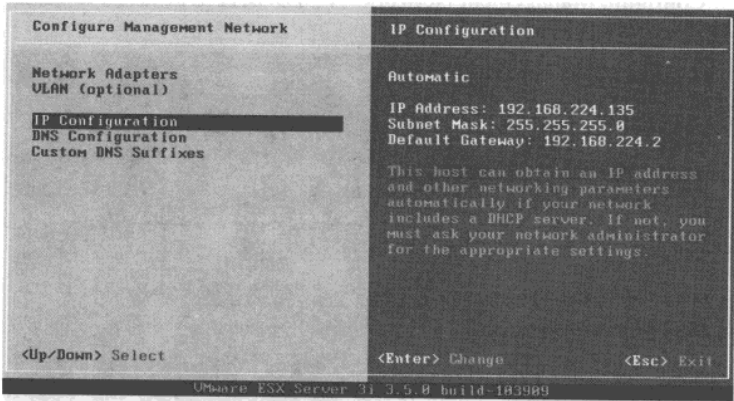


图 5-138 设置 IP 地址

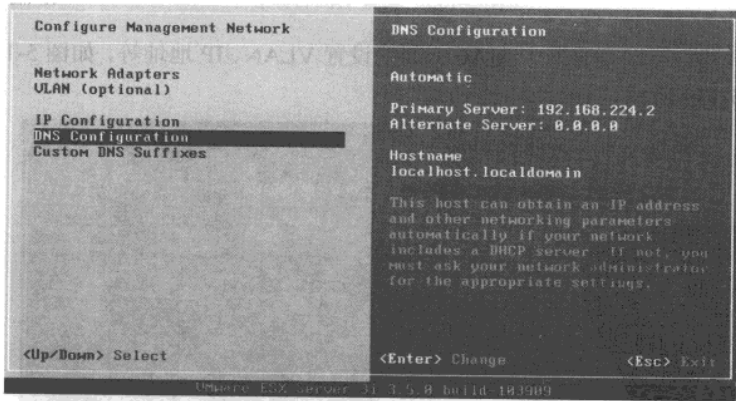


图 5-139 设置 DNS 地址

设置完成后，按 ESC 键返回图 5-140 所示界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

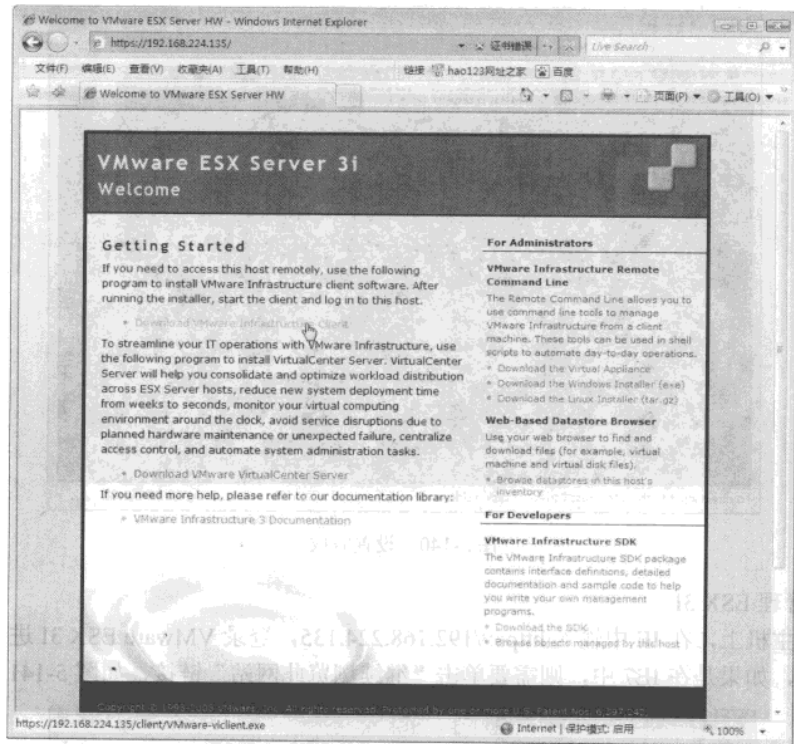


图 5-142 下载 VMware 管理工具

第 3 步，下载之后，安装该管理工具，如图 5-143 所示。

第 4 步，在“VMware Infrastructure Client”界面，输入 VMware ESX 3i 的地址、ROOT 用户及密码，如图 5-144 所示。

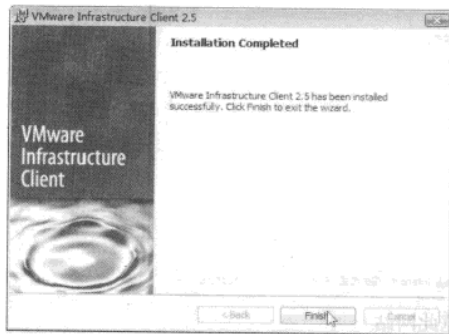


图 5-143 安装管理工具

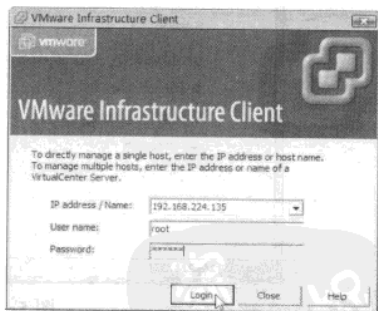


图 5-144 连接到 VMware ESX 3i

(3) 在 VMware ESX 3i 中创建虚拟机。

第 1 步，连接到 ESX 3i 后，如图 5-145 所示。用鼠标右键单击“localhost localdomain”选项，从弹出的快捷菜单中选择“New Virtual Machine”命令。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

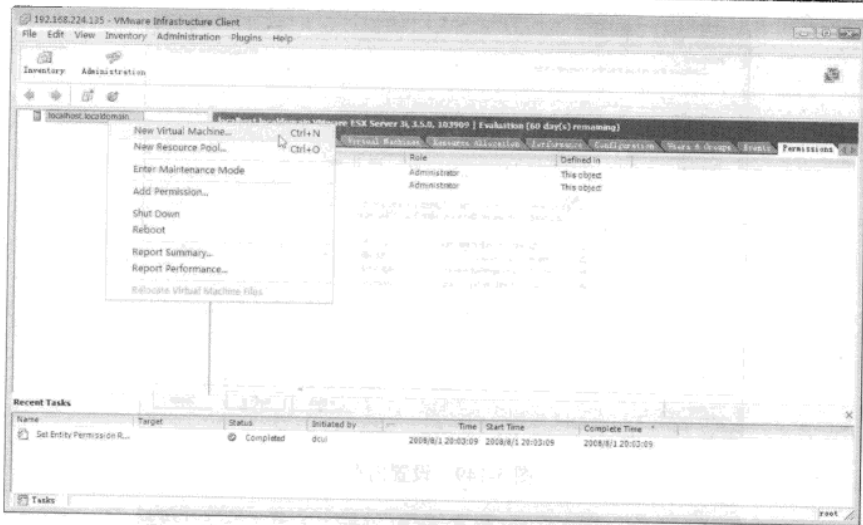


图 5-145 创建虚拟机

第 2 步，创建虚拟机的过程与在 VMware Workstation 中相类似，如图 5-146～图 5-155 所示。

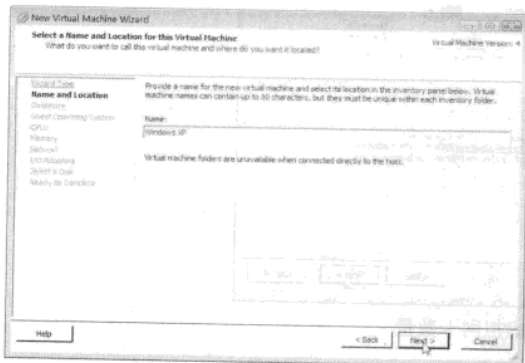


图 5-146 设置虚拟机名称

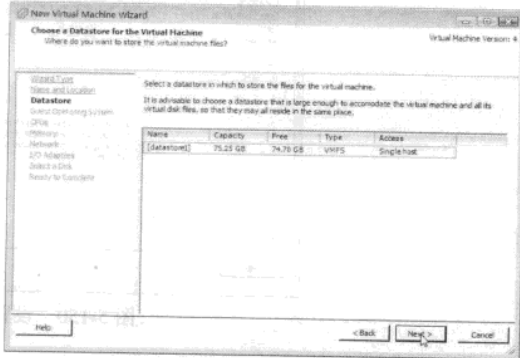


图 5-147 选择保存虚拟机的位置

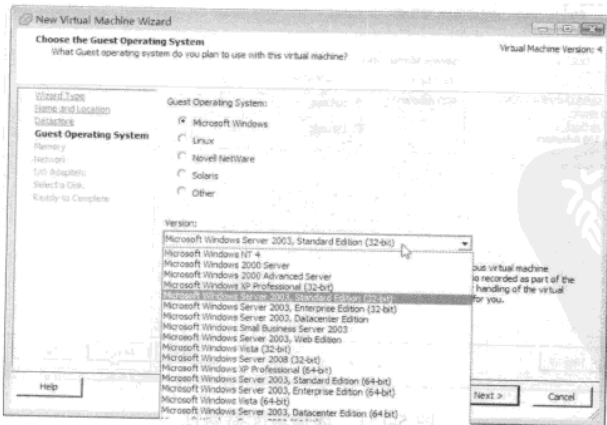


图 5-148 选择客户操作系统

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

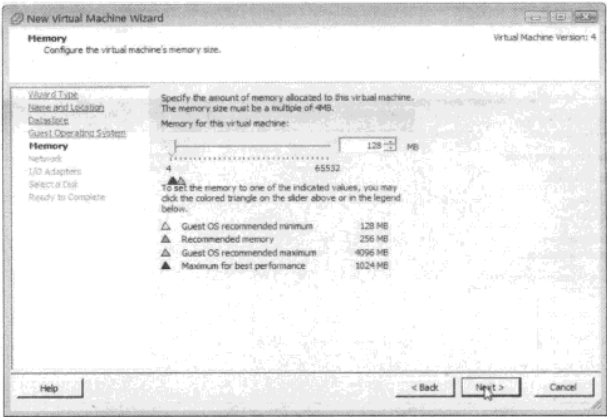


图 5-149 设置内存

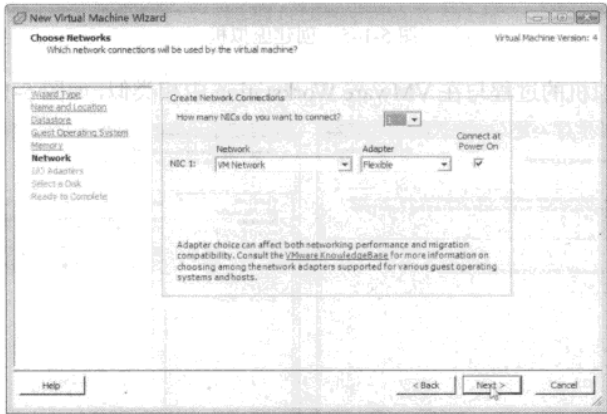


图 5-150 设置虚拟网卡数量

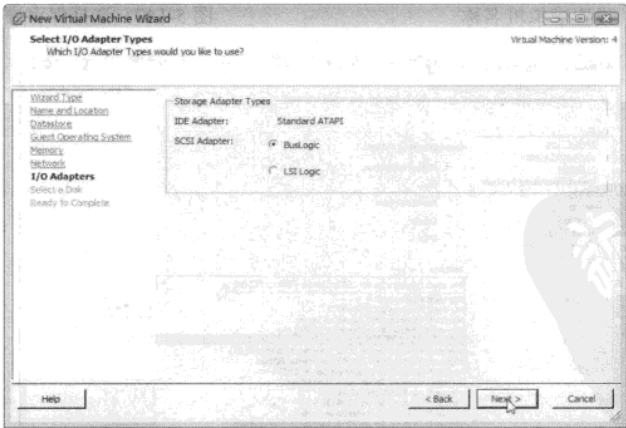


图 5-151 选择适配器属性

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

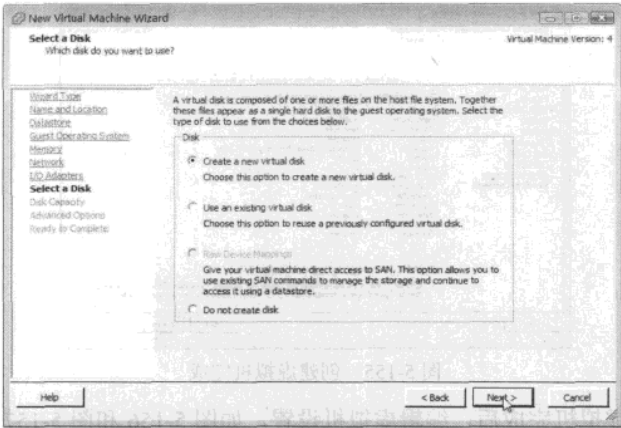


图 5-152 创建新虚拟硬盘

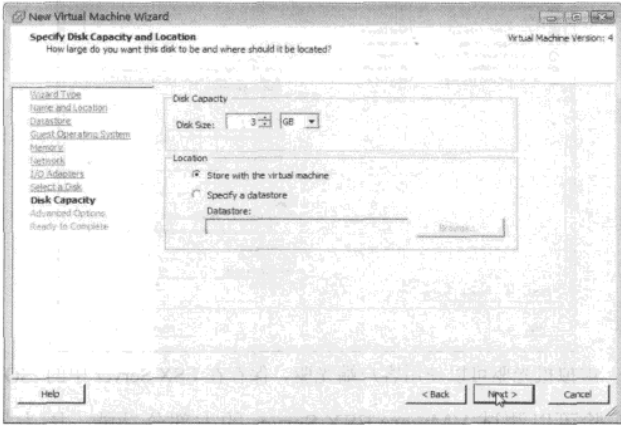


图 5-153 分配 3 GB 内存

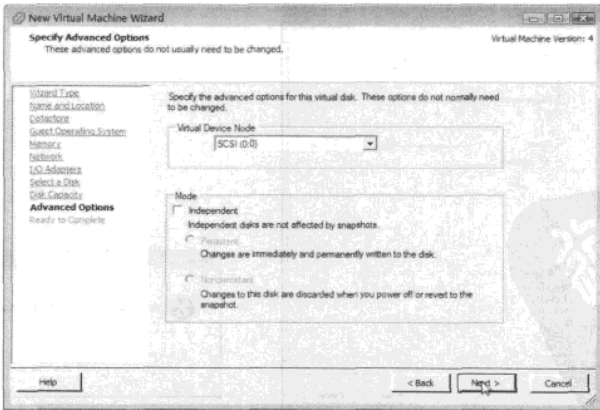


图 5-154 设置虚拟 SCSI 结点

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

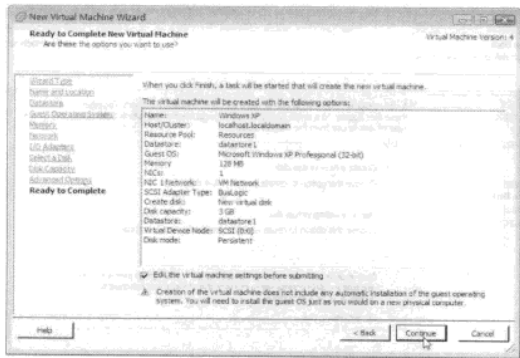


图 5-155 创建虚拟机完成

第 3 步，创建虚拟机完成后，编辑虚拟机设置，如图 5-156 和图 5-157 所示。

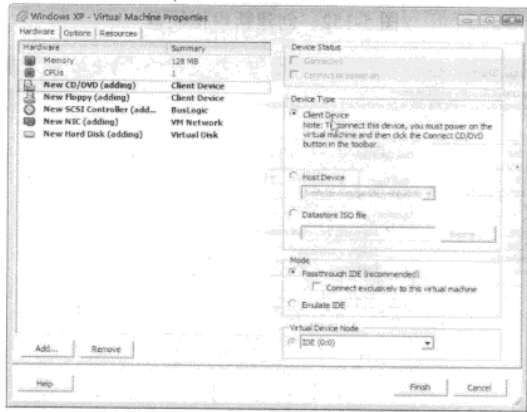


图 5-156 虚拟机光驱可以使用客户端光驱、保存在 ESX Server 中的 ISO 镜像图

第 4 步，本次实验可以测试 VMware ESX Server 的大部分功能，因为是在虚拟机中做的，所以不能在此启动虚拟机。如果尝试启动虚拟机，则会弹出图 5-158 的提示。

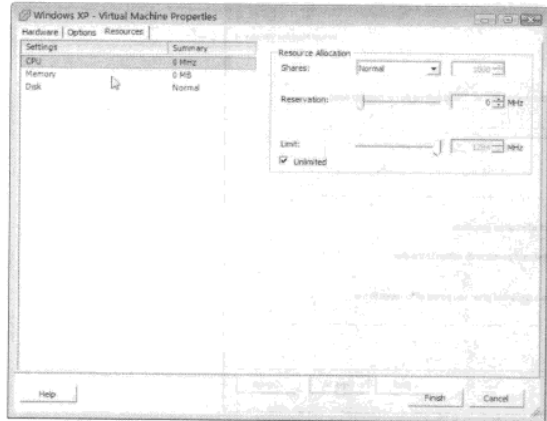


图 5-157 设置 CPU、内存资源

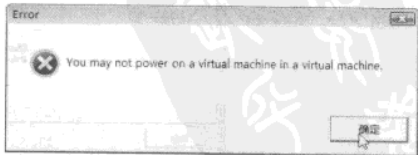


图 5-158 不能在虚拟机中打开虚拟机的电源

第 6 章 操作系统方面

作为一个称职的网络管理员除了具备网络维护及安全方面的能力、服务器管理等经验，以及熟练使用网络管理工具之外还应具备一定解决操作系统方面的问题的能力。本章分别从计算机故障，工作站操作系统及服务器操作系统等方面对经常遇到的问题做了一些总结。

6.1 计算机故障解决经验

计算机无法正常启动、电脑黑屏和计算机出现蓝屏都是在使用过程中经常会遇到的问题。普通用户可以不去考虑其产生故障的原因和解决方法，但作为合格的网络管理员就不能说出现了问题就丢给维修站不管了，很多情况是网管员来处理的。本节就以上 3 个现象分别做了详细的总结，另外本节还对排除其他计算机故障做了一些经验小总结。

6.1.1 计算机无法启动故障解决经验

Windows XP 系统的计算机无法启动的故障解决方法：

（1）使用 Windows 启动盘启动计算机。

如果启动问题是由于活动分区的启动记录或者操作系统启动所使用的文件被破坏造成的，启动盘就能够解决问题。具体方法如下：

创建 Windows 启动盘，找一台配置相似、工作正常的 Windows XP 计算机，打开“我的电脑”，单击鼠标右键选择磁盘图标，然后在后续的菜单中选择“格式化”。当“格式化”对话框出现以后，保留所有默认设置，然后单击“开始”按钮。当格式化操作完成后，关闭“格式化”对话框返回到 My Computer，双击 C：驱的图标，访问根目录，将 Boot.ini、NTLDR、Ntdetect.com 三个文件复制到磁盘上。创建好了 Windows 启动盘之后，将它插入故障系统的驱动器内，按 Ctrl+Alt+Delete 组合键重新启动计算机。

（2）使用最后一次的正确配置来启动计算机。

你还可以尝试用最后一次正确配置来启动操作系统。该功能可以让你取消任何在注册表 CurrentControlSet 键上做出的、导致问题的修改，这个键是定义硬件和驱动器设置的。Known Good Configuration 功能用系统最后一次正常启动的 CurrentControlSet 键值来取代当前的键值。具体方法如下：

首先按 Ctrl+Alt+Delete 组合键，重新启动计算机。当你看到屏幕上出现“Please select the operating system to start”，或者听到计算机发出一声蜂鸣声，按 F8 键，屏幕上就会出现 Windows 高级选项菜单。从菜单中选择“Last Known Good Configuration”选项，然后按 Enter 键。要记住，你只有一次机会会使用 Last Known Good Configuration 功能。

（3）进行系统恢复来启动计算机。

能够帮助解决 Windows XP 启动问题的另一个工具是系统恢复。系统恢复作为一项服务在

网管天下 网管经验谈

后台运行，并且持续监视重要系统组件的变化。当它发现一项改变即将发生时，系统恢复会立即在变化发生之前，为这些重要组件做一个名为恢复点的备份复制，而且系统恢复默认的设置是每 24 个小时创建恢复点。具体方法如下：

首先按 **Ctrl+Alt+Delete** 组合键，重新启动计算机。当你看到屏幕上出现 “Please select the operating system to start”，或者听到计算机发出一声蜂鸣声，按 **F8** 键，屏幕上就会出现 Windows 高级选项菜单。现在从菜单中选择安全模式，然后按 **Enter** 键。当 Windows XP 进入安全模式之后，单击“开始”按钮，选择所有程序附件系统工具菜单，选择系统恢复。单击“下一步”按钮，选择一个恢复点，启动恢复程序。

（4）使用 Recovery Console 启动计算机。

如果 Windows XP 启动问题比较严重。你可以使用 Windows XP CD 启动系统，然后使用一个名为恢复控制台的工具。具体做法如下：

在故障计算机的 CD-ROM 驱动器中插入 Windows XP CD，然后按 **Ctrl+Alt+Delete** 组合键重新启动计算机。一旦系统从 CD 上启动后，只要根据提示就能够很容易地加载启动所需要的基本文件。当你看到 **Welcome To Setup** 界面的时候，按 **R** 键进入 **Recovery Console**。然后你就会看到 **Recovery Console** 菜单。它显示了包含操作系统文件的文件夹，并提示你选择打算登录的操作系统。你需要在键盘上输入菜单上的序号，然后系统会提示你输入管理员密码，你就会进入主 **Recovery Console** 提示页面。

（5）修复被破坏的 Boot.ini 启动计算机。

随着 Windows XP 操作系统的加载，**Ntldr** 程序指向 **Boot.ini** 文件，以确定操作系统文件的位置，以及选择哪个启动选项。所以如果 **Boot.ini** 文件出了问题，Windows XP 系统就不能启动了。你可以使用恢复控制台特殊版本的 **Bootcfg** 工具来修复它。当然，你必须首先用 Windows XP CD 重新启动系统，按照（4）中的介绍打开 **Recovery Console**。你可以这样调用 **Bootcfg** 工具：在 **Recovery Console** 命令提示符后，输入 **Bootcfg /parameter** 在这里的 **/parameter** 是这些需要的参数之一。

/Add：扫描所有的 Windows 安装，帮助你向 **Boot.ini** 文件中增加任何新的内容。

6.1.2 电脑黑屏解决方法

1. 硬件篇

（1）检查电脑部件是否安插牢靠。

首先请检查显示器电缆是否牢固可靠地插入到主机接口中，然后再检查显卡与主板 I/O 插槽之间的接触是否良好。如有必要，请将显卡取下，重新安插一次，确保安插到位，接触良好。

（2）确认显示器是否损坏。

如果显示器和显卡安装牢靠，那么请换一台确认正常的显示器试一试。如果不再黑屏，那么原因是显示器可能损坏了。

（3）确认风扇是否有问题。

如果显示器未损坏，请进一步检查 CPU 风扇是否运转。如运转，可用万用表测量电压输出是否正常为 $\pm 12V$ 、 $\pm 15V$ ，若不正常可以换一个电源试一试。

（4）检测 CPU、显卡和内存条。

如仍出现黑屏，则可将除 CPU、显卡、内存条之外的所有组件取下，然后加电启动电脑。如果内存有故障，应会有报警声。如果不是内存原因，请换一个正常的 CPU，开机重新检测。如仍出现黑屏，则只能换一个主板了，问题也应该出现在主板上。

除了硬件方面的原因引起黑屏现象外，也有以下三个方面的“软”原因可能会引发“黑屏”。

■ 2. 软件篇

（1）硬件加速设置过高。

硬件加速可以使得要处理大量图形的软件运行得更加流畅，但是如果电脑硬件加速设置得过高，则可能导致“黑屏”现象。为解决“黑屏”故障，请首先尝试降低硬件加速。

第 1 步，单击“开始”按钮，选择“控制面板”，然后双击“显示”图标。

第 2 步，打开“疑难解答”选项卡，在“硬件加速”下，将滑块从“全”逐渐拖动到接近“无”的位置。

第 3 步，单击“确定”按钮。

（2）禁用 3D 加速或升级显卡驱动程序。

如果 Windows 已为 3D 加速进行了配置，但显卡却不支持该功能，那么当运行游戏或多媒体程序时，可能会出现“黑屏”故障。

第 1 步，单击“开始”按钮，选择“运行”，然后在“打开”框中输入“dxdiag”，并按下 Enter 键。

第 2 步，打开“显示”选项卡，在“DirectX 功能”下单击“测试 Direct 3D”按钮，以获得正确的 Direct 3D 功能。

第 3 步，如果屏幕中没有出现一个旋转的立方体，则表明显卡不支持 3D 加速。此时，请单击“Direct 3D 加速”后的“禁用”按钮，以禁用该功能。

如果你的显卡不支持 3D 加速，除禁用该功能外，你还可与显卡生产厂商联系，更新驱动程序，以使其支持 DirectX 的 3D 加速。

（3）显卡的驱动程序与显卡不兼容。

DirectX 安装程序可能会错误地检测显卡，并安装不能正常驱动的驱动程序，请确认使用的显卡驱动程序是否正确。

第 1 步，单击“开始”按钮，选择“控制面板”，然后双击“系统”图标。

第 2 步，打开“硬件”选项卡，单击“设备管理器”按钮，然后单击“显示卡”或者“显示适配器”前的“+”号，再右键单击其下的显示适配器，在弹出的快捷菜单中选择“属性”命令。

第 3 步，打开“驱动程序”选项卡，单击“驱动程序详细资料”按钮，以显示所使用的显卡驱动程序。如果所使用的驱动程序与显卡不兼容，那么请你在“驱动程序”选项卡中，单击“更新驱动程序”按钮，然后按屏幕指示操作，安装显卡新版本的驱动程序。

电脑死机的 4 种原因：

① 开机过程中出现死机：在启动计算机时，只听到硬盘自检声而看不到屏幕显示，或干脆在开机自检时发出鸣叫声，但计算机不工作、或在开机自检时出现错误提示等。

② 在启动计算机操作系统时发生死机：屏幕显示计算机自检通过，但在装入操作系统时，

网管天下 网管经验谈

计算机出现死机的情况。

③ 在使用一些应用程序过程中出现死机：计算机一直都运行良好，只在执行某些应用程序时出现死机的情况。

④ 退出操作系统时出现死机：就是在退出 Win98 等系统或返回 DOS 状态时出现死机。由于在“死机”状态下无法用软件或工具对系统进行诊断，因而增加了故障排除的难度。死机的一般表现有：系统不能启动、显示黑屏、显示“凝固”、键盘不能输入、软件运行非正常中断等。

死机的原因有两个方面：一是由电脑硬件引起的，二是软件设计不完善或与系统和系统其他正在运行的程序发生冲突。

在硬件方面，原因就是近来在电脑 DIY 界流行的“超频”，让 CPU 工作在额定运行频率以外的时钟频率上，CPU 处于超额工作状态，出现死机就不奇怪了；其次一个原因是某个硬件过热，或者硬件资源冲突，当然还有其他一些硬件方面的原因。

在软件方面，因为软件原因而造成的死机在电脑中几乎占了大多数（超频了的电脑除外）。在 Windows9x 系列中使用了 16 位和 32 位混合的内核模式，因此安全性很低，因程序内存冲突而死机是经常会发生的事情。下面就来介绍一下遇到死机故障后一般的检查处理方法。

（4）排除系统“假”死机现象。

首先，排除因电源问题带来的“假”死机现象。应检查电脑电源是否插好，电源插座是否接触良好，主机、显示器和打印机、扫描仪、外置式 MODEM，音箱等主要外接电源的设备电源插头是否可靠地插入了电源插座、上述各部件的电源开关是否都处于开（ON）的状态。

其次，检查电脑各部件间数据控制连线是否连接正确和可靠，插头间是否有松动现象。尤其是主机与显示器的数据线连接不良常常造成“黑屏”的假死机现象。

（5）排除病毒感染引起的死机现象。

用无毒干净的系统盘引导系统，然后运行 KILL，AV9（5）SCAN 等防病毒软件的最新版本对硬盘进行检查，确保电脑安全，排除因病毒引起的死机现象。

另外，如果在杀毒后引起了死机现象，这多半是因为病毒破坏了系统文件、应用程序及关键的数据文件，或是杀毒软件在消除病毒的同时对正常的文件进行了误操作，破坏了正常文件的结构。碰到这类问题，只能将被损坏（即运行时引起死机）的系统或软件重装。

（6）软件安装、配置问题引起的死机现象分析与排除。

首先，如果是在软件安装过程中死机，则可能是系统某些配置与安装的软件冲突。这些配置包括系统 BIOS 设置、CONFIGSYS 和 AUTOEXEC.BAT 的设置、WIN.INI、SYSTEM.INI 的设置，以及一些硬件驱动程序和内存驻留程序的设置。

可以试着修改上述设置项。对 BIOS 可以取其默认设置，如“LOAD SETUP DEFAULT”和“LOAD BIOS DEFAULT”；对 CONFIGSYS 和 AUTOEXEC.BAT 则可以在启动时按 F5 键跳过系统配置文件或按 F8 键逐步选择执行，以及逐项修改 CONFIGSYS 和 AUTOEXEC.BAT 中的配置（尤其是 EMM386 中关于 EMS、XMS 的配置情况）来判断硬件与安装程序什么地方发生了冲突，对于一些硬件驱动程序和内存驻留程序，则可以通过不装载它们的方法来避免冲突。

其次，如果是在软件安装后发生了死机，则是安装好的程序与系统发生了冲突。一般的做法是恢复系统在安装前的各项配置，然后分析安装程序新装入部分使用的资源和可能发生的冲突，逐步排除故障原因。删除新安装程序也是解决冲突的方法之一。

(7) 系统启动过程中的死机现象来分析。

系统启动过程中的死机现象包括两种情况：

① 致命性死机，即系统自检过程未完成就死机，一般系统不给出提示。对此可以根据开机自检时致命性错误列表的情况，再结合其他方法对故障原因做进一步的分析。

② 非致命性死机，在自检过程中或自检完成后死机，但系统给出声音、文字等提示信息。可以根据开机自检时非致命性错误代码表和开机自检时鸣笛音响对应的错误代码表来检查：开机自检时鸣笛音响对应的错误代码表中所列的情况，是对可能出现故障的部件做重点检查，但也不能忽略相关部件的检查，因为相当多的故障并不是由提示信息指出的部件直接引起，而常常由相关部件故障引发。

(8) 因使用、维护不当引起的死机现象分析与排除。

电脑在使用一段时间后也可能因为使用、维护不当而引起死机，尤其是长时间不使用电脑后常会出现此类故障。引起的原因有以下几种：

① 积尘导致系统死机：灰尘是电脑的大敌。过多的灰尘附着在 CPU、芯片、风扇的表面会导致这些元件散热不良，电路印刷板上的灰尘在潮湿的环境中常常导致短路。上述两种情况均会导致死机。

具体处理方法可以用毛刷将灰尘扫去，或用棉签沾无水酒精清洗积尘元件。注意不要将毛刷和棉签的毛、棉留在电路板和元件上而成为新的死机故障源。

② 部件受潮：长时间不使用电脑，会导致部分元件受潮而不能正常使用。可用电吹风的低热挡均匀对受潮元件“烘干”。注意不可对元件一部分加热太久或温度太高，避免烤坏元件。

③ 板卡、芯片引脚氧化导致接触不良：将板卡、芯片拔出，用橡皮擦轻轻擦拭引脚表面去除氧化物，重新插入插座。

④ 板卡、外设接口松动导致死机：仔细检查各 I/O 插槽插接是否正确，各外设接口接触是否良好，线缆连接是否正常。

(9) 因系统配置不当引起的死机现象分析。

① 主频设置不当：此类故障主要有 CPU 主频跳线开关设置错误、Remark 的 CPU 引起的 BIOS 设置与实际情况不符、超频使用 CPU，或 CPU 性能不良死机。

② 内存条参数设置不当：此类故障主要有内存条设置错误和 Remark 内存条引起的 BIOS 设置与实际情况不符。

③ CACHE 参数设置不当：此类故障主要有 CHCCE 设置错误、RemarkCACHE 引起的 BIOS 设置与实际情况不符。

④ CMOS 参数被破坏：频繁修改 CMOS 参数，或病毒对 CMOS 参数的破坏，常常会导致 CMOS 参数混乱而很难恢复。可以采用对 CMOS 放电的方法并采用系统 BIOS 默认设置值重新设定 CMOS 参数。CMOS 的放电方法可参照主板说明书进行。如果是病毒感染引起的，在重设 CMOS 参数后，还必须对硬盘杀毒。

(10) 硬件安装不当引起的死机现象与排除。

硬件外设安装过程中的疏忽常常导致莫名其妙的死机，而且这一现象往往在电脑使用一段时间后才逐步显露出来，因而具有一定的迷惑性。

① 部件安装不到位、插接松动、连线不正确引起的死机。显示卡与 I/O 插槽接触不良常常引起显示方面的死机故障，如“黑屏”，内存条、CACHE 与插槽插接松动则常常引起程序运行中死机、甚至系统不能启动，其他板卡与插槽（插座）的接触问题也常常引起各种死机现

网管天下 网管经验谈

象。要排除这些故障，只须将相应板卡、芯片用手摁紧、或从插槽（插座）上拔下重新安装。如果有空闲插槽（插座），也可将该部件换一个插槽（插座）安装以解决接触问题。线缆连接不正确有时也会引发死机故障。

② 安装不当导致部件变形、损坏引起的死机：口径不正确、长度不恰当的螺钉常常导致部件安装孔损坏，螺钉接触到部件内部电路引起短路导致死机；不规范的主板、零部件或不规范的安装步骤常常引起机箱、主板、板卡外形上的变异，因而挤压该部件内部元件导致局部短路、内部元件损坏从而发生莫名其妙的死机。如果只是电脑部件外观变形，可以通过正确的安装方法和更换符合规格的零部件来解决；如果已经导致内部元件损坏，则只能更换新的零部件了。

（11）硬件质量问题引起的死机现象分析与排除。

一般说来，电脑产品都是国际大厂商按照国际标准流水线生产出来的，部件不良率是很低的。但是高利润的诱惑使许多非法厂商对电脑标准零部件改头换面、进行改频、重新标记（Remark）、以次充好甚至将废品、次品当做正品出售，导致这些“超水平”发挥的产品性能不稳定，环境略有不适或使用时间稍长就会频繁发生故障。尤其是 CPU、内存条、主板等核心部件及其相关产品的品质不良，是导致无原因死机的主要故障源。应着重检查以下部件：

① CPU。CPU 是被假冒得最多也是极容易导致死机的部件。被 Remark 的 CPU 在低温、短时间使用时一切正常，但只要在连续高温的环境中长时间使用，其死机弊端就很容易暴露。使用 Windows、3DS 等对 CPU 特性要求较高的软件比 DOS 等简单软件更能发现 CPU 的问题。如需确认是否为此故障，可参照说明书将 CPU 主频调低 1~2 档次使用，比如将 166 降为 150、133 或 120 使用。如果死机现象大幅度减少或消失，就可以判断是 CPU 有问题。也可以用交换法，更换同型号的正常 CPU，如果不再死机一般可以断定是 CPU 的问题。有些用户喜欢把 CPU 超频使用以获得高速的性能，这也是常导致计算机死机的原因。一般将 CPU 跳回原频率就能解决死机问题。

② 内存条。内存条常常被做的手脚有：速度标记被更改。如：70 ns 被 Remark 为 60 ns，非奇偶校验冒充奇偶校验内存，非 EDO 内存冒充 EDO 内存，劣质内存条冒充好内存条。在 BIOS 中将内存条读写时间适当增加（如：从 60 ns 升为 70 ns），如果死机消失可以断定是内存条速度问题。如果是内存本身的质量问题，只有更换新的内存条才能解决。

③ 主板。一般主板的故障常常是最先考虑，然而却是要到最后才能确定的。除了印刷板上的飞线、断线和主板上元件被烧焦、主板受挤压变形、主板与机箱短路等明显的现象外，主板本身的故障只有在确认了主板上所有零部件正常（将你的板卡、CPU、内存条等配件拿到好的主板上使用正常，而别人使用正常的板卡、器件插到你的主板上就不能正常运行）时才能判断是否是主板故障，如果更换了好的同型号主板死机依然存在，则可能是该主板与某个零部件不兼容。要么更换兼容的其他型号的主板、要么只能用拔插法依次测试各板卡、芯片，找出不兼容的零部件更换之。

④ 电源、风扇、机箱等。劣质电源、电源线缆故障、电源插接松动、电源电压不稳都是引起不明原因死机的罪魁祸首。CPU 风扇、电源风扇转动不正常、风扇功率不足则会引起 CPU 和机箱内“产热大户”元件散热不良而引起死机。

（12）系统黑屏故障的排除。

系统死机故障多半表现为黑屏（即显示器屏幕上无任何显示），这类故障与显示器、显示卡关系很密切，同时系统主板、CPU、CACHE、内存条和电源等部件的故障也能导致黑屏。

系统黑屏死机故障的一般检查方法如下：

① 排除“假”黑屏：检查显示器电源插头是否插好，电源开关是否已打开，显示器与主机上显示卡的数据连线是否连接好、连接插头是否松动，看是否是因为这些因素而引起的黑屏。另外，应该动一下鼠标或按一下键盘看屏幕是否恢复正常。因为黑屏也可能是因为设置了节能模式（可在 BIOS 设置中查看和修改）而出现的假死机。

② 在黑屏的同时系统其他部分是否工作正常，如：启动时软 / 硬盘驱动器自检是否通过、键盘按键是否有反应等。可以通过交换法用一台好的显示器接在主机上测试、如果只是显示器黑屏而其他部分正常，则只是显示器出了问题，这仍是一种假死机现象。

③ 黑屏发生在显示驱动程序安装或显示模式设置期间，显然是选择了显示系统不能支持的模式，应选择一种较基本的显示方式。如：Windows 下设置显示模式后黑屏或花屏，则应在 DOS 下运行 Windows 目录下的 SETUP.EXE 程序选择标准 VGA 显示方式。

④ 检查显示卡与主板 I/O 插槽接触是否正常、可靠，必要时可以换一个 I/O 槽插入显示卡试试。

⑤ 换一块已确认性能良好的同型号显示卡插入主机重新启动，若黑屏死机现象消除则是显示卡的问题。

⑥ 换一块已确认性能良好的其他型号显示卡插入主机重新启动，若黑屏死机现象消除则是显示卡与主机不兼容，可以考虑更换显示卡或主板。

⑦ 检查是否错误设置了系统的核心部件，如 CPU 的频率、内存条的读写时间、CACHE 的刷新方式、主板的总线速率等，这些都可能导致黑屏死机。

⑧ 检查主机内部各部件连线是否正确，有一些特殊的连线错误会导致黑屏死机。

(13) 找出显示器黑屏故障的原因。

开机后显示器黑屏，无显示，是许多计算机用户经常遇到的问题。其实，只要你对计算机的工作原理有一定的了解，这些非器件损坏的简单故障完全可以自己动手排除。

(1) 当显示器黑屏没有图像显示时（不过目前市面上的显示器在主机没有信号送来时，屏幕上会显示器“没有信号线连接”），首先检查主机电源是否插接良好，电源的风扇是否转动？主机面板上电源指示灯、硬盘指示灯是否闪亮？因为若主机电源不工作或主板没有供电时，显示器在没有接收到信号时，当然就不会有图像显示的。

(2) 再检查显示器的电源是否插接良好？如果你的显示器的电源开关是轻触开关时，当你给显示器加电时，应该会听到轻微的“辟啪”声，这时可判断显示器的开关电源电路良好。再检查显示器的电源开关是否已经开启？显示器的电源指示灯是否亮？当用手靠近显示器屏幕并慢慢移动是否有“滋滋”的声音，同时手上的汗毛有被吸起的感觉，这是在检查显示器高压电路是否正常工作了。

(3) 如果确定显示器已经加电了，且有高压产生时，继续检查显示器的数据线接头与显卡的信号输出接口是否接触良好？是否有松动？再拔下插头检查一下，D 型接口中是否有弯曲和断针或者有大量污垢。这是许多用户经常遇到的问题，在连接 D 型插口时，用力不均匀，或忘记拧紧接口的固定螺丝，使接口松动造成接触不良，或因安装时方法不当或用力过大，使 D 型接口内有断针或弯针，以致造成接触不良。

网管天下 网管经验谈

注 意

显示器的数据线插头的 15 针可能有缺针，如 4，9，11 针，这是正常的，千万不要人为的用其他金属丝来补充这些缺针位，以免造成其他故障。1，2，3 针为红，绿，蓝三种信号输入，如果哪根针接触不好时，屏幕就会缺少相应的颜色。

(4) 打开机箱检查显卡安装是否正确？与主板插槽是否接触良好？显卡或插槽是否因使用时间太长而积尘太多，以至造成接触不良？显卡上的芯片是否有烧焦、开裂的痕迹。当因显卡原因导致黑屏时，计算机开机自检时即有一短四长的“嘀嘀”声提示。安装显卡时，要用手握住显卡上半部分，均匀用力插入卡槽中，使显卡的固定螺丝口与主机箱的螺丝口吻合。未插正时不要强行固定，以免造成显卡扭曲。如果确认安装正确时，可以取下显卡用酒精棉球擦拭一下插脚的金属或者换一个插槽（只能对于 PCI 显卡）安装。如果还不行，只能换一块好的显卡试一下。

如果还不行，在确定显卡完好时，还要考虑显卡与主板的兼容性。最好查一下相关的资料或问一下网友。

(5) 检查其他的板卡（包括声卡、解压卡、视频捕捉卡）与主板的插槽接触是否良好？注意检查硬盘的数据线与硬盘的电源线接法是否正确？更换其他板卡的插槽，清洗插脚。这一点许多人往往容易忽视。一般认为，计算机黑屏是显示器和显卡问题，与其他设备无关。实际上，因为声卡等设备的安装不正确，导致系统初使化难以完成，特别是硬盘的数据线与硬盘电源线插错，容易造成无显示的故障。

(6) 检查内存条与主板的接触是否良好？把内存条重新插拔一次或者换个插槽试试，又或者更换新的内存条。如果内存条出现问题，计算机在启动时，会有连续急促的“嘀嘀”声。提示音会因为主板不同而不同。

(7) 检查 CPU 与主板上的 CPU 座接触是否良好？因搬动或其他因素，是否使 CPU 与 SLOT1 插口或 SOCKET370 插座接触不良。最好用手按一按 CPU 或取下 CPU 再重新安装一次。

(8) 检查 CPU 外频，倍频，内存的频率等的跳线或 CMOS 中的设置是否正确。对照主板说明书，逐一检查相关跳线，顺序为“CPU 外频跳线—CPU 倍频跳线—内存频率跳线”。

(9) 检查 CPU 的电压是否设置恰当。设置 CPU 电压跳线时要小心，一定要与 CPU 的工作电压相符。(8) 和 (9) 这两步对于一些组装机或喜欢超频的用户在出现黑屏时要仔细检查。

(10) 检查 CMOS 参数设置是否正确。如果你的电脑装有两个显卡，你在 CMOS 里设置的是第一个初始化 PCI 显卡，而你的唯一的显示器接在 AGP 显卡上，当然显示器是不会亮的。

(11) 检查主机和显示器所要求的工作环境是否符合？工作电压是否正常，环境温度是不是过高等。除了按上述步骤进行检查外，还可以根据计算机的工作状况来快速定位，如在开启主机电源后，可听见“嘀”的一声表示计算机自检完成，如果此时硬盘指示灯不停地闪烁，则应在 (2) 至 (4) 检查。

(12) 如果显示器在计算机启动过程中有内容显示，只是在加载 WIN98 的画面后出现黑屏时，这就只是 WIN98 系统软件方面的问题了。

上述的检查方法是基于显示器本身无电源故障，即开启主机电源后显示器的电源指示灯由绿变黄但显示器黑屏没有图像显示。如果使用上述步骤显示器仍然无显示，应请专业人员维修。

6.1.3 | Windows 蓝屏错误代码小结

在 Windows 提供给用户快捷的操作时，也会出现一些令用户感到无奈的问题，其中就有出现频率比较高的“蓝屏”故障，在“蓝屏”故障中有一故障代码，通过它可以确定引起故障的原因，本节就跟大家分享一下蓝屏代码汇总及其解释：

- 0x0000 作业完成。
- 0x0001 不正确的函数。
- 0x0002 系统找不到指定的档案。
- 0x0003 系统找不到指定的路径。
- 0x0004 系统无法开启档案。
- 0x0005 拒绝存取。
- 0x0006 无效的代码。
- 0x0007 储存体控制区块已毁。
- 0x0008 储存体空间不足，无法处理这个指令。
- 0x0009 储存体控制区块地址无效。
- 0x000A 环境不正确。
- 0x000B 尝试加载一个格式错误的程序。
- 0x000C 存取码错误。
- 0x000D 资料错误。
- 0x000E 储存体空间不够，无法完成这项作业。
- 0x000F 系统找不到指定的磁盘驱动器。
- 0x0010 无法移除目录。
- 0x0011 系统无法将档案移到其他的磁盘驱动器。
- 0x0012 没有任何档案。
- 0x0013 储存媒体为写保护状态。
- 0x0014 系统找不到指定的装置。
- 0x0015 装置尚未就绪。
- 0x0016 装置无法识别指令。
- 0x0017 资料错误（cyclic redundancy check）
- 0x0018 程序发出一个长度错误的指令。
- 0x0019 磁盘驱动器在磁盘找不到指定的扇区或磁道。
- 0x001A 指定的磁盘或磁盘无法存取。
- 0x001B 磁盘驱动器找不到要求的扇区。
- 0x001C 打印机没有纸。
- 0x001D 系统无法将资料写入指定的磁盘驱动器。
- 0x001E 系统无法读取指定的装置。
- 0x001F 连接到系统的某个装置没有作用。
- 0x0020 这个程序正在被另一个程序占用，暂时不能启用。
- 0x0021 档案的一部份被锁定，现在无法存取。

网管天下 网管经验谈

- 0x0022 磁盘驱动器的磁盘不正确。请将%2（Volume Serial Number: %3）插入磁盘机%1。
- 0x0024 开启的分享档案数量太多。
- 0x0026 到达档案结尾。
- 0x0027 磁盘已满。
- 0x0032 不支持这种网络要求。
- 0x0033 远程计算机无法使用。
- 0x0034 网络名称重复。
- 0x0035 网络路径找不到。
- 0x0036 网络忙碌中。
- 0x0037 这个具体的网卡资源或驱动不可用。
- 0x0038 这块网卡的 BIOS 设置受限。
- 0x0039 网络配接卡发生问题。
- 0x003A 指定的服务器无法执行要求的作业。
- 0x003B 网络发生意外错误。
- 0x003C 远程配接卡不兼容。
- 0x003D 打印机队列已满。
- 0x003E 服务器的空间无法储存等候打印的档案。
- 0x003F 等候打印的档案已经删除。
- 0x0040 指定的网络名称无法使用。
- 0x0041 拒绝存取网络。
- 0x0041 拒绝存取网络。
- 0x0042 网络资源类型错误。
- 0x0043 网络名称找不到。
- 0x0044 超过区域计算机网络配接卡的名称限制。
- 0x0045 超过网络 BIOS 作业阶段的限制。
- 0x0046 远程服务器已经暂停或者正在起始中。
- 0x0047 由于联机数目已达上限，此时无法再联机到这台远程计算机。
- 0x0048 指定的打印机或磁盘装置已经暂停作用。
- 0x0050 档案已经存在。
- 0x0052 无法建立目录或档案。
- 0x0053 INT 24 失败
- 0x0054 处理这项要求的储存体无法使用。
- 0x0055 近端装置名称已经在使用中。
- 0x0056 指定的网络密码错误。
- 0x0057 参数错误。
- 0x0058 网络发生资料写入错误。
- 0x0059 此时系统无法执行其他行程。
- 0x0064 无法建立其他的系统 semaphore。
- 0x0065 属于其他行程专用的 semaphore
- 0x0066 semaphore 已经设定，而且无法关闭。

- 0x0067 无法指定 semaphore。
- 0x0068 在岔断时间无法要求专用的 semaphore。
- 0x0068 在岔断时间无法要求专用的 semaphore。
- 0x0069 此 semaphore 先前的拥有权已经结束。
- 0x006A 请将磁盘插入%1。
- 0x006B 因为代用的磁盘尚未插入，所以程序已经停止。
- 0x006C 磁盘正在使用中或被锁定。
- 0x006D Pipe 已经中止。
- 0x006E 系统无法开启指定的装置或档案。
- 0x006F 档名太长。
- 0x0070 磁盘空间不足。
- 0x0071 没有可用的内部档案标识符。
- 0x0072 目标内部档案标识符不正确。
- 0x0075 由应用程序所执行的 IOCTL 呼叫不正确。
- 0x0076 写入验证参数值不正确。
- 0x0077 系统不支持所要求的指令。
- 0x0078 此项功能仅在 Win32 模式有效。
- 0x0079 semaphore 超过逾时期间。
- 0x007A 传到系统呼叫的资料区域太小。
- 0x007B 文件名、目录名称或储存体卷标语法错误。
- 0x007C 系统呼叫层次不正确。
- 0x007D 磁盘没有设定卷标。
- 0x007E 找不到指定的模块。
- 0x007F 找不到指定的程序。
- 0x0080 没有子行程可供等待。
- 0x0080 没有子行程可供等待。
- 0x0081 %1 这个应用程序无法在 Win32 模式下执行。
- 0x0082 一个操作是尝试把一个应用文件应用到一个打开的硬盘扇区上或者是一个 I/O 的硬件通道上。
- 0x0083 尝试将档案指针移至档案开头之前。
- 0x0084 无法在指定的装置或档案，设定档案指针。
- 0x0085 JOIN 或 SUBST 指令无法用于内含事先结合过的磁盘驱动器。
- 0x0086 尝试在已经结合的磁盘驱动器，使用 JOIN 或 SUBST 指令。
- 0x0087 尝试在已经替换的磁盘驱动器，使用 JOIN 或 SUBST 指令。
- 0x0088 系统尝试删除未连结过的磁盘驱动器的连结关系。
- 0x0089 系统尝试删除未替换过的磁盘驱动器的替换关系。
- 0x008A 系统尝试将磁盘驱动器结合到已经结合过之磁盘驱动器的目录。
- 0x008B 系统尝试将磁盘驱动器替换成已经替换过之磁盘驱动器的目录。
- 0x008C 系统尝试将磁盘驱动器替换成已经替换过之磁盘驱动器的目录。
- 0x008D 系统尝试将磁盘驱动器 SUBST 成已结合的磁盘驱动器的目录。

网管天下 网管经验谈

0x008E 系统此刻无法执行 JOIN 或 SUBST。
0x008F 系统无法将磁盘驱动器结合或替换同一磁盘驱动器下目录。
0x0090 这个目录不是根目录的子目录。
0x0091 目录仍有资料。
0x0092 指定的路径已经被替换过。
0x0093 资源不足，无法处理这项指令。
0x0094 指定的路径这时候无法使用。
0x0094 指定的路径这时候无法使用。
0x0095 尝试要结合或替换的磁盘驱动器目录，是已经替换过的目标。
0x0096 CONFIG.SYS 文件未指定系统追踪信息，或是追踪功能被取消。
0x0097 指定的 semaphore 事件 DosMuxSemWait 数目不正确。
0x0098 DosMuxSemWait 没有执行；设定太多的 semaphore。
0x0099 DosMuxSemWait 清单不正确。
0x009A 你所输入的储存媒体标识无长度限制。
0x009B 无法建立其他的执行绪。
0x009C 接收行程拒绝接受信号。
0x009D 区段已经被舍弃，无法被锁定。
0x009E 区段已经解除锁定。
0x009F 执行绪识别码的地址不正确。
0x00A0 传到 DosExecPgm 的自变量字符串不正确。
0x00A1 指定的路径不正确。
0x00A2 信号等候处理。
0x00A4 系统无法建立执行绪。
0x00A7 无法锁定档案的部份范围。
0x00AA 所要求的资源正在使用中。
0x00AD 取消范围的锁定要求不明显。
0x00AE 档案系统不支持自动变更锁定类型。
0x00B4 系统发现不正确的区段号码。
0x00B6 操作系统无法执行 %1。
0x00B7 档案已存在，无法建立同一档案。
0x00BA 传送的旗号错误。
0x00BB 指定的系统旗号找不到。
0x00BC 操作系统无法执行 %1。
0x00BD 操作系统无法执行 %1。
0x00BE 操作系统无法执行 %1。
0x00BF 无法在 Win32 模式下执行 %1。
0x00C0 操作系统无法执行 %1。
0x00C1 %1 不是正确的 Win32 应用程序。
0x00C2 操作系统无法执行 %1。
0x00C3 操作系统无法执行 %1。

0x00C4 操作系统无法执行这个应用程序。

0x00C5 操作系统目前无法执行这个应用程序。

0x00C6 操作系统无法执行 %1。

0x00C7 操作系统无法执行这个应用程序。

6.1.4 | 电脑故障排除经验

相对于其他电器产品来说，电脑是一个容易出这样那样故障的电器。电脑故障，是许多电脑爱好者头痛的事情，该如何来应对及解决所遇到的电脑故障呢？在此作者总结撰写了一篇电脑维护中的“八先八后”法则，抛砖引玉，以飨读者。

(1) 先调查，后熟悉。

无论是对自己的电脑还是别人的电脑进行维修，首先要弄清故障发生时电脑的使用状况及以前的维修状况，才能对症下药。此外，在对电脑进行维修前还应了解清楚电脑的软硬件配置及已使用年限等，做到有的放矢。

实例解析：

电脑在使用中频繁出现系统死机与“非法操作”提示十分恼人，该用户准备重新格式化磁盘重装操作系统。作者觉得不用这么麻烦，作者仔细看了其电脑的配置与软硬件安装情况并用杀毒软件查毒后……经作者询问，该用户称最近安装了新版的 IE6 浏览器，会不会是 IE6 浏览器与其系统兼容性不好呢？作者尝试在“添加 / 删除程序”栏里卸载掉新版的 IE6 浏览器，重新启动电脑后，故障现象不再频繁发生。

(2) 先机外，后机内。

对于出现主机或显示器不亮等故障的电脑，应先检查机箱及显示器的外部件，特别是机外的一些开关、旋钮是否调整外部的引线、插座有无断路、短路现象等，不要认为这些是无关紧要的小处，实践证明许多用户的电脑故障都是由此而起的。当确认机外部件正常时，再打开机箱或显示器进行检查。

实例解析：

电脑在搬动位置后出现主机不亮（主机风扇也不转）的故障，该用户认为是主机电源年久失修被损毁，打开机箱准备拆下电源更换。作者观察其主机和显示器分别用一根电源线从电源插座连接，而显示器显示正常。本着先简单后复杂的原则先将主机的电源插头换一个电源插孔试之，无效，便将正常使用的显示器电源线取下连接主机，主机恢复正常。将问题线接上显示器，也不亮，证明问题就来自这看似不起眼的电源线（内部断路）。

(3) 先机械，后电气。

对于光驱及打印机等外设而言，先检查其有无机械故障再检查其有无电气故障，是检修电脑的一般原则。例如 CD 光驱不读盘，应当先分清是机械原因引起的（如或光头的问题），还是由电气毛病造成的。只有当确定各部位转动机构及光头无故障时，再进行电气方面的检查。

实例解析：

已购一年多的 40 速光驱，故障现象为读不出盘。拆开光驱先观察一下光驱的内部结构状况，此款光驱为全钢结构，一般应不会存在较严重的机械情况，所以不应急于在它的光头和加大激光头功率上进一步“摧残”它。先放进一张碟片，仔细的观察了一下碟片的旋转及光头组件的动作，快进等电机的进退情况，发现碟片的旋转基本正常，电机的进退也没太大问题，反

网管天下 网管经验谈

而光头组件在空载或加碟片的情况下，在滑动杆上滑动十分吃力，关掉电源，用手轻轻推了几下光头组件使其在杆上滑动，有很明显的迟滞感。这时作者再重点观察这款光驱的滑动杆，见其上边原本应白色的润滑油已变成了浅黑色，拿到光线较强的地方甚至可见密密的灰尘杂质，难怪滑动不灵活了。先用纯酒精将滑动组件上的已含杂质的润滑油清理干净，然后再重新加上新的润滑油，然后重新试机，读盘恢复正常。

（4）先软件，后硬件。

先排除软件故障再排除硬件问题，这是电脑维修中的重要原则。例如 Windows 系统软件的被损坏或丢失可能造成死机故障的产生，因为系统启动是一步一个脚印的过程，哪一个环节都不能出现错误，如果存在损坏的执行文件或驱动程序，系统就会僵死在这里。但电脑各部件的本身问题，插接件的接口接触不良问题，硬件设备的设置问题，驱动程序是否完善，与系统的兼容性，硬件供电设备的稳定性，以及各部件间的兼容性抗外界干扰性，等等。也有可能引发电脑硬件死机故障的产生，在维修时应先从软件的方面着手再考虑硬件的方面。

实例解析：

一台电脑启动自检后，在屏幕上显示“No ROMBasic, System Halted”信息后死机，硬盘灯也长亮不熄。排除了硬盘坏道的原因，很明显造成这一故障的原因是硬盘的引导程序被破坏，造成系统找不到硬盘而死机。修复这种故障的办法很多，如可采用 KV300，它能很轻松的解决硬盘引导区被破坏的故障，其使用方法很简单。读者可参考下 KV300 的说明文件，作者在此就不多介绍了。而如果没有 KV3000，那么也可用软盘启动电脑后，在纯 DOS 状态下执行特别的“FDISK / MBR”命令，也可强行将正确的主引导程序及结束标识覆盖在硬盘的主引导区上，但需要注意的是这个命令有一定的危险性。

（5）先清洁，后检修。

在检查机箱内部配件时，应先着重看看机内是否清洁，如果发现机内各元件、引线、走线及金手指之间有尘土、污物、蛛网或多余焊锡、焊油等，应先加以清除，再进行检修，这样既可减少自然故障，又可取得事半功倍的效果。实践表明，许多故障都是由于脏污引起的，一经清洁故障往往会自动消失。

实例解析：

一台电脑在打开机箱安装一新显卡后，出现重新开机后显示器黑屏，机内喇叭发出连续的长声“嘀嘀”蜂鸣报警声。故障分析：机箱内喇叭发出连续的鸣叫，这是典型的内存报错故障。虽然说你在拆机或搬动电脑时有可能并没有去动内存条，但是内存是个精密部件，它的大敌就是灰尘，而你的电脑在使用一段时间之后机箱内就很可能铺上薄薄一层余灰，而和 CPU 靠得较近的内存便是最大的“受害者”，CPU 风扇很可能给你的内存上铺上厚厚一层灰尘，稍有震动灰尘就有可能掉入内存插槽里，引起局部短路或接触不良，造成电脑启动时显示器黑屏和机箱内喇叭报错。对于这种情况，你应该先检查内存的安装情况，可用手先按几下内存再开机，看其接触是否变好，如还不行；那么你可以将内存条取下，先将内存条表面的灰尘打扫干净，然后再用小号细毛刷仔仔细细将内存插槽内的灰尘清扫干净，然后重新插好内存条故障一般就可排除。

（6）先电源，后计算机。

电源是计算机及配件的心脏，如果电源不正常，就不可能保证其他部分的正常工作，也就无从检查别的故障。根据经验，电源部分的故障率在机中占的比例最高，许多故障往往就是由电源引起的，所以先检修电源常能收到事半功倍的效果。

实例解析：

一电脑在更换主板重新启动电脑后，出现电源灯亮但系统不自检、显示器黑屏的故障。打开机箱，仔细观察，发现 CPU 风扇正常运转，关掉电源后仔细检查板卡的安装，重点重新安装内存条及显卡，检查主板的相关跳线等情况，确认无误，遂采用“最小系统法”排除故障，去掉硬盘光驱等的连接线，只保持主板，CPU，内存，显卡的最小系统，开机后系统顺利开启。于是重点检查光驱和硬盘的连接情况，当上好光驱后上述故障重新出现，难道是光驱没上好？该光驱单独接在 IDE2 总线接口上，作者检查发现，该光驱连接用的 IDE 线接头上无防反插的凸块，难道是接反了？仔细一看果不其然，正确上好后系统正常。

(7) 先外围，后内部。

在检查电脑或配件的重要元器件时，不要先急于更换或对其内部的重要配件动手，而应检查其外围电路，在确认外围电路正常时，再考虑更换配件或重要元器件。若不问青红皂白，一味更换配件或重要元器件了事，只能造成不必要的损失。从维修实践可知，配件或重要元器件外围电路或机械的故障远高于其内部电路。

实例解析：

一单位里的 PC 硬盘在正常使用中，只是重新启动了一下电脑后，硬盘便找不到了，据该电脑的工作人员称，这硬盘前两天也曾出现这样的毛病，但过了一会儿自己又找得到了。打开机箱一看该硬盘为三年前购的西数 3.2 GB 硬盘，由于经常被拆卸下来复制数据显得很旧。对于这类故障可首先检查 IDE 硬盘线，换新后无效，试着换个电源插头重新插紧，开机后硬盘“忽忽”的转动起来恢复正常。装好配件合上机箱盖板，再重启，奇怪的是硬盘又不见了踪影……。

如此反复几次，硬盘无法正常使用，但作者只要将硬盘电源线插拔几次，便又能恢复正常。会不会是硬盘电源接口内的接线柱有接触不良，取下观察，并无生锈或起卤现象。用万用表来检测接线柱与硬盘电路板上的接线柱焊点间的导通情况，作者发现有一根柱（5V）要用表笔抵紧才能导通，排除了接线柱表面氧化或焊点虚焊等情况，作者花 3 元购来一电源线转接线，剪去接头剥出铜线，将其一一按顺序在硬盘电源部分电源插口接线柱在电路板上的对应焊点上——焊好，将电源转接线的公头插上主机电源线的一个母头，重新开机，PC 又恢复了往日的正常。

6.2 操作系统方面问题解决经验

相对计算机故障来说操作系统出现问题的情况会更多一点，像内存不能读写、虚拟内存不足等应该说是使用计算机的人都遇到过的现象。本节就以上两个现象出现的原因及解决经验分别做了详细的总结。另外操作系统出现问题很多情况是可以通过对进程的管理和分析解决的，所以本节还对操作系统中常用的进程的解析和在命令行下对进程的管理经验做了一些总结。本节最后对如何修改应用程序访问权限做了一些介绍，以达到对某些应用程序起到保护作用的目的。

6.2.1 内存不能够读写问题的分析与解决

近期，一些朋友总提出内存不能为“read”或者“written”的问题，鉴于产生这些问题的原因多样复杂，判断和处理这些问题比较麻烦，现在将网上找到的这篇较为全面的资料，加上

网管天下 网管经验谈

自己收集到的部分例子奉上，供大家共享。

问题：

运行某些程序的时候，有时会出现内存错误的提示，然后该程序就关闭。

“0x???????” 指令引用的“0x???????”内存。该内存不能为“read”。

“0x???????” 指令引用的“0x???????”内存，该内存不能为“written”。

一般出现这个现象有两方面的原因，一是硬件，即内存方面有问题，二是软件，这就有多方面的问题了。

故障分析。

硬件方面：一般来说，内存出现问题的可能性并不大，主要原因是：内存条坏了、内存质量有问题，还有就是两个不同牌子不同容量的内存混插，也比较容易出现不兼容的情况，同时还要注意散热问题，特别是超频后。你可以使用 MemTest 这个软件来检测一下内存，它可以彻底的检测出内存的稳定度。

假如是双内存，而且是不同品牌的内存条混插或者买了二手内存时，一旦出现问题，就要检查是不是内存的问题，或者是和其他硬件不兼容。

软件方面：先简单说说原理：内存有个存放数据的地方叫缓冲区，当程序把数据放在某一位置时，因为没有足够空间，就会发生溢出现象。举个例子：一个桶子只能装一斤的水，当放入两斤的水进入时，就会溢出来，而系统则是在屏幕上表现出来。这个问题，经常出现在 Windows2000 和 XP 系统上，Windows 2000/XP 对硬件的要求是很苛刻的，一旦遇到资源死锁、溢出或者类似 Windows 98 里的非法操作，系统为保持稳定，就会出现上述情况。另外也可能是硬件设备之间的兼容性不好造成的。

几个典型故障例子及解决办法：

例一：打开 IE 浏览器或者没过几分钟，就会出现“0x70dcf39f”指令引用的“0x00000000”内存，该内存不能为“read”。要终止程序，请单击“确定”的信息框，单击“确定”后，又出现“发生内部错误，你正在使用的其中一个窗口即将关闭”的信息框，关闭该提示信息后，IE 浏览器也被关闭。

解决方法：修复或升级 IE 浏览器，同时打上补丁。看过其中一个修复方法是，Win2000 自升级，也就是 Win2000 升级到 Win2000，其实这种方法也就是把系统还原到系统初始的状态下。比如你的 IE 升级到了 6.0，自升级后，会被 IE5.0 代替。

例二：在 Windows xp 下双击光盘里面的“AutoRun.exe”文件，显示“0x77f745cc”指令引用的“0x00000078”内存。该内存不能为“written”，要终止程序，请单击“确定”，而在 Windows 98 里运行却正常。

解决方法：这可能是系统的兼容性问题，WinXP 的系统，右键单击“AutoRun.exe”文件，在弹出的快捷菜单中选择“属性”命令，打开“兼容性”选项卡，把“用兼容模式运行这个程序”项选择上，并选择“Windows 98/Me”。Win2000 如果打了 SP 的补丁后，只要开始运行，输入：regsvr32 c:\winnt\apppatch\slayerui.dll。右键单击，属性，也会出现兼容性的选项。

例三：RealOne Gold 关闭时出现错误，以前一直使用正常，最近却在每次关闭时出现“0xffffffff”指令引用的“0xffffffff”内存。该内存不能为“read”的提示。

解决方法：当使用的输入法为微软拼音输入法 2003，并且隐藏语言栏时（不隐藏时没问题）关闭 RealOne 就会出现这个问题，因此在关闭 RealOne 之前，可以显示语言栏或者将任意其他输入法作为当前输入法来解决这个问题。

操作系统方面 | 6

例四：我的豪杰超级解霸自从上网后就不能播放了，每次都提示“0x060692f6”（每次变化）指令引用的“0xff000011”内存不能为“read”，终止程序请按确定。

解决方法：试试重装豪杰超级解霸，如果重装后还会出现同样的问题，到官方网站下载相应版本的补丁试试。还不行，只好换就用别的播放器试试了。

例五：双击一个游戏的快捷方式，“0x77f5cd0”指令引用“0xffffffff”内存，该内存不能为“read”，并且提示 Client.dat 程序错误。

解决方法：重装显卡的最新驱动程序，然后下载并且安装 DirectX9.0。

例六：一位朋友发信息过来，我的电脑便出现了错误信息：“0*772b548f”指令引用的“0*00303033”内存，该内存不能为“written”，然后 QQ 自动下线，而再打开 QQ，发现了他发过来的十几条的信息。

解决方法：这是对方利用 QQ 的 BUG，发送特殊的代码，应该是 QQ 出错，只要打上补丁或升级到最新版本，就没事了。

例七：我的笔记本电脑用的 XP 系统，有时关闭网页时会弹出 tbrowser.exe 遇到问题需要关闭，然后有弹出 0x03e7c738 指令引用的 0x03e7c738 内存，该内存不能为 read，请问是怎么回事？

解决方法：先查杀一下病毒，另外如果你安装了浏览增强之类的软件，请卸掉。

例八：从桌面或开始菜单中打开任何一个程序，出现错误提示：“0x.....”指令引用的“0x00000000”内存，该内存不能为“read”。省略号代表可变值，而从运行中打开程序没问题。

解决方法：运行 regedit 进入注册表，在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks 下，应该只有一个正常的键值{AEB6717E-7E19-11d0-97EE-00C04FD91972}，将其他的删除（默认键值当然不要删除）。

例九：我三个月前配了台机子。系统比较不稳定，三个月内已经重装过多次系统，四五天前刚装过系统，可是经常随机地出现 Explorer-应用程序错误，“0x4a01259d”指令引用的“0x00000000”内存。该内存不能为“read”。要终止程序，请单击“确定”按钮。要调试程序，请单击“取消”按钮。如果单击“确定”按钮，Windows 桌面就不见了。这种问题在之前的系统也出现过，不知道是不是硬件的问题？

解决方法：内存的兼容性问题！遇到这类问题，用户可以自行打开计算机把内存的位置调动一下，看问题是否可以解决，如果问题依旧，可与你的朋友调换内存使用。

通过上面的几个例子，可以看到，出现故障的原因有好多种，下面列出已经提到和有可能发生的原因，方便查阅。

问题产生原因解决方法：

- (1) 内存条坏了 更换内存条。
- (2) 双内存不兼容 使用同品牌的内存或只用一块内存。
- (3) 内存质量问题 更换内存条。
- (4) 散热问题 加强机箱内部的散热。
- (5) 内存和主板没插好或和其他硬件不兼容等 重插内存或换个插槽。
- (6) 硬盘有问题 更换硬盘。
- (7) 驱动问题 重装驱动。如果是新系统，要先安装主板驱动。
- (8) 软件损坏 重装软件。
- (9) 软件有 BUG 打补丁或用最新的版本。

网管天下 网管经验谈

- (10) 软件和系统不兼容 给软件打上补丁或者试试系统的兼容模式。
 - (11) 软件和软件之间有冲突 如果最近安装了什么新软件，卸载了试试。
 - (12) 软件要使用到其他相关的软件有问题 重装相关软件。比如播放某一格式的文件时出错，可能是这个文件的解码器有问题。
 - (13) 病毒问题，杀毒。
 - (14) 杀毒软件与系统或软件冲突 由于杀毒软件是进入底层监控系统的，可能与一些软件冲突，卸载了试试。
 - (15) 系统本身有问题。
- 有时候操作系统本身也会有 BUG，要注意安装官方发行的升级程序，像 SP 的补丁，最好要打上。如果还不行就只能重装系统或更换其他版本的系统了。

Windows 系统出现内存错误。

使用 Windows 操作系统的人有时会遇到这样的错误信息，“0X????????指令引用的 0x00000000 内存，该内存不能 written”，然后应用程序被关闭。如果去请教一些“高手”，得到的回答往往是“Windows 就是这样不稳定”之类的说辞。其实，这个错误并不一定是 Windows 不稳定造成的。本文就来简单分析这种错误的常见原因。

1. 应用程序没有检查内存分配失败

程序需要一块内存用以保存数据时，就需要调用操作系统提供的“功能函数”来申请，如果内存分配成功，函数就会将新开辟的内存区地址返回给应用程序，应用程序就可以通过这个地址使用这块内存。这就是“动态内存分配”，内存地址也就是编程中的“指针”。

内存不是永远都招之即来、用之不尽的，有时候内存分配也会失败。当分配失败时系统函数会返回一个 0 值，这时返回值“0”已不表示新启用的指针，而是系统向应用程序发出的一个通知，告知出现了错误。作为应用程序，在每一次申请内存后都应该检查返回值是否为 0，如果是，则意味着出现了故障，应该采取一些措施挽救，这就增强了程序的“健壮性”。

若应用程序没有检查这个错误，它就会按照“思维惯性”认为这个值是给它分配的可用指针，继续在之后的运行中使用这块内存。真正的 0 地址内存区保存的是计算机系统中最重要“中断描述符表”，绝对不允许应用程序使用。在没有保护机制的操作系统下（如 DOS），写数据到这个地址会导致立即死机，而在健壮的操作系统中，如 Windows 等，这个操作会马上被系统的保护机制捕获，其结果就是由操作系统强行关闭出错的应用程序，以防止其错误扩大。这时候，就会出现上述的“写内存”错误，并指出被引用的内存地址为“0x00000000”。

内存分配失败故障的原因很多，内存不够、系统函数的版本不匹配等都可能有影响。因此，这种分配失败多见于操作系统使用很长时间后，安装了多种应用程序（包括无意中“安装”的病毒程序），更改了大量的系统参数和系统文件之后。

2. 应用程序由于自身 BUG 引用了不正常的内存指针

在使用动态分配的应用程序中，有时会有这样的情况出现：程序试图读写一块“应该可用”的内存，但不知为什么，这个预料中可用的指针已经失效了。有可能是“忘记了”向操作系统要求分配，也可能是程序自己在某个时候已经注销了这块内存而“没有留意”等。注销了的内存被系统回收，其访问权已经不属于该应用程序，因此读写操作也同样会触发系统的保护机制，企图“违法”的程序唯一的下场就是被操作终止运行，回收全部资源。计算机世界的法律还是

要比人类有效和严厉得多。

像这样的情况都属于程序自身的 BUG，你往往可在特定的操作顺序下重现错误。无效指针不一定总是 0，因此错误提示中的内存地址也不一定为“0x00000000”，而是其他随机数字。

如果系统经常有以上所提到的错误提示，下面的建议可能会有帮助。

- (1) 查看系统中是否有木马或病毒。这类程序为了控制系统往往不负责任地修改系统，从而导致操作系统异常。平常应加强信息安全意识，对来源不明的可执行程序绝不好奇。
- (2) 更新操作系统，让操作系统的安装程序重新复制正确版本的系统文件、修正系统参数。有时候操作系统本身也会有 BUG，要注意安装官方发行的升级程序。
- (3) 试用新版本的应用程序。

6.2.2 虚拟内存不足的原因汇总及解决方法

(1) 虚拟内存设置的太小。

第 1 步，把鼠标移动到桌面的“我的电脑”图标上单击右键，在弹出的快捷菜单中“属性”命令，然后弹出“系统属性”对话框，打开“高级”选项卡，如图 6-1 所示。

第 2 步，在对话框中的“性能”栏中，单击“设置”按钮，弹出“性能选项”对话框，如图 6-2 所示。

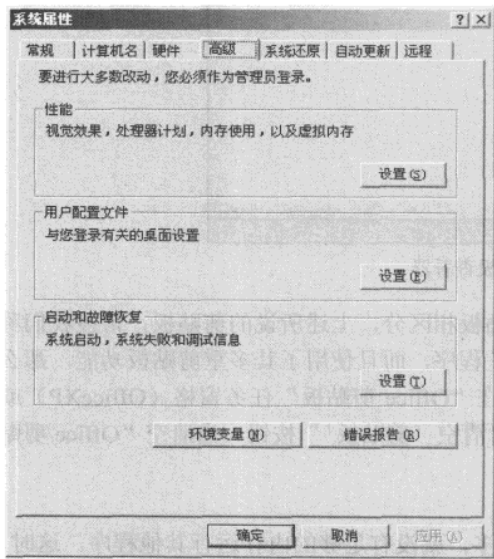


图 6-1 “高级”选项卡

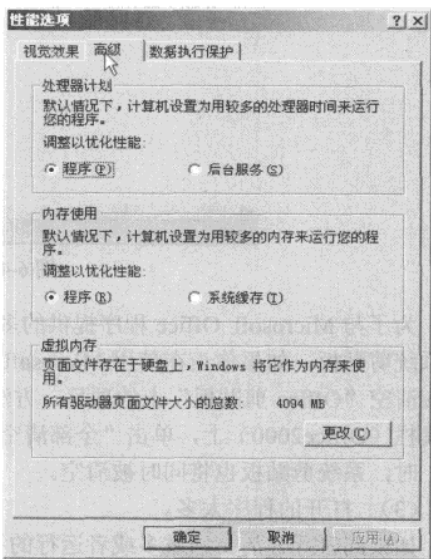


图 6-2 “性能选项”对话框

第 3 步，在“性能选项”对话框的最下面“虚拟内存”栏里单击“更改”按钮，弹出“虚拟内存”对话框，在对话框中选择你要设置虚拟内存的硬盘（你的哪个分区的剩余空间多你就选哪个分区，也可以同时选多个分区）选择“E”盘。选中“自定义大小”单选按钮，在“初始大小”文本框中输入适当的数，此处为 800，最大值为 1024。然后再单击下面的“设置”按钮，单击“确定”按钮。

网管天下 网管经验谈

第4步，返回到“性能选项”对话框，单击“确定”按钮又返回到“系统属性”对话框中，再单击“确定”按钮就会关闭系统属性对话框，如此设置就全部完成了。

（2）剪贴板占用内存。

实际上，剪贴板是内存中的一块临时区域，当你在程序中使用了“复制”或“剪切”命令后，Windows 将把复制或剪切的内容及其格式等信息暂时存储在剪贴板上，以供“粘贴”使用。如果当前剪贴板中存放的是一幅图画，则剪贴板就占用了不少的内存。这时，请按下述步骤清除剪贴板中的内容，释放其占用的内存资源。

单击“开始”按钮，选择“运行”选项，输入“clipbrd”，单击“确定”按钮，如图 6-3 所示。

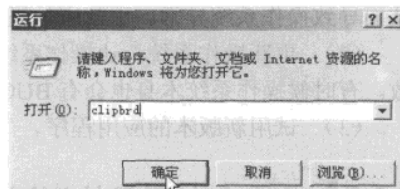


图 6-3 打开剪贴板查看器

调出剪贴板查看器程序，如图 6-4 所示。

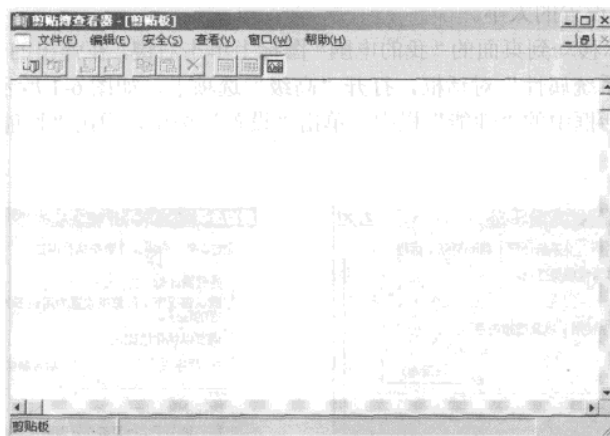


图 6-4 剪贴板查看器

为了与 Microsoft Office 程序提供的多重剪贴板相区分，上述所说的剪贴板，常被我们称为系统剪贴板。如果你正在使用 Microsoft Office 程序，而且使用了其多重剪贴板功能，那么你应该清空“Office 剪贴板”上的项目，方法是：在“Office 剪贴板”任务窗格（OfficeXP）或工具栏（Office2000）上，单击“全部清空”或“清空‘剪贴板’”按钮。当清空“Office 剪贴板”时，系统剪贴板也将同时被清空。

（3）打开的程序太多。

如果同时打开的文档过多或者运行的程序过多，就没有足够的内存运行其他程序。这时，对于多文档界面（MDI）程序，如 Word、Excel 等，请关闭当前文档外的所有文档，并退出当前未使用的程序，然后或许你就能够继续执行因“内存不足”而被中断的任务。

（4）重新启动计算机。

如果只退出程序，并不重新启动计算机，程序可能无法将内存资源归还给系统。请重新启动计算机以释放系统资源，然后再次运行程序或执行被中断的任务。

（5）自动运行的程序太多。

如果在启动 Windows 时自动运行的程序太多，那么，即使重新启动计算机，也没足够的

内存用来运行其他程序。所以要确定设置为自动运行的程序是否太多。

第 1 步，单击“开始”按钮，选择“运行”选项。输入“msconfig”，单击“确定”按钮，如图 6-5 所示。

打开“系统配置实用程序”对话框，如图 6-6 所示。

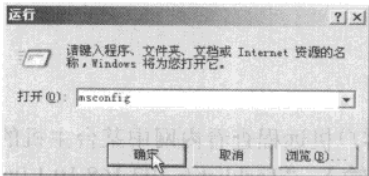


图 6-5 打开系统配置实用程序

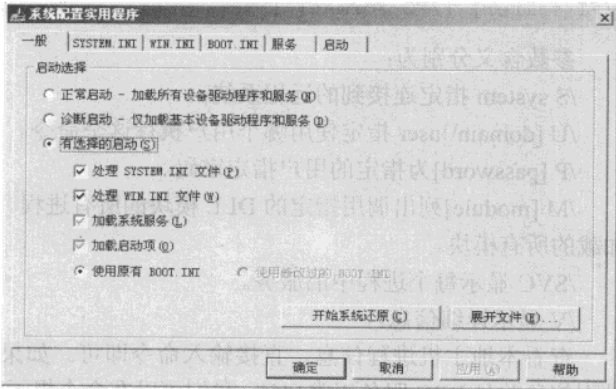


图 6-6 系统配置实用程序

第 2 步，打开“一般”选项卡，取消“处理 WIN.INI 文件”复选框，如图 6-7 所示。

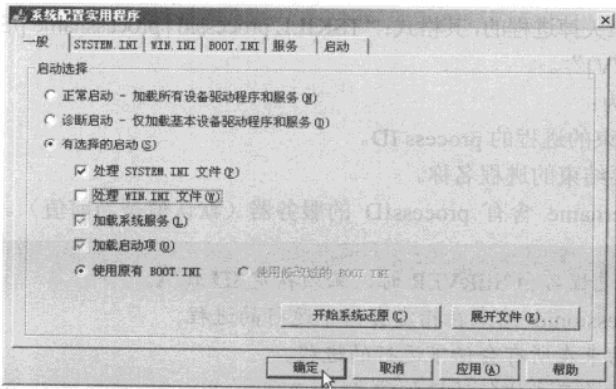


图 6-7 取消“处理 WIN.INI 文件”复选框

第 3 步，单击“确定”按钮，当系统提示重新启动计算机时，请单击“是”按钮。重新启动计算机后，如果内存不足的问题已经解决，你就可以将计算机配置为启动时不打开任何程序。

6.2.3 Windows 命令行下的进程管理小经验

相信大多数网管员都有用命令行（CMD）解决问题的习惯，本节就介绍一下 Windows 命令行下的进程管理的小经验。进程的管理无非就两步：一是查看进程，二是关闭不正常的进程。所以要跟大家介绍的就是这方面的 3 个命令。

网管天下 网管经验谈

(1) Tasklist.

这个命令用来显示运行在本地或远程计算机上的所有进程，可以监控用户的操作。其格式：

```
Tasklist [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH].
```

参数含义分别为：

/S system 指定连接到的远程系统。

/U [domain\]user 指定使用哪个用户执行这个命令。

/P [password]为指定的用户指定密码。

/M [module]列出调用指定的 DLL 模块的所有进程。如果没有指定模块名，显示每个进程加载的所有模块。

/SVC 显示每个进程中的服务。

/V 显示详细信息。

查看本地主机进程信息，直接输入命令即可。如果从客户机远程查看内网中某台主机的进程信息并且 RPC 服务正常启动，我们可以在命令提示符下输入：“Tasklist /s 192.168.10.1 0/u administrator /p password”其中“192.168.10.10”为该主机内网 IP 地址，“administrator”为该主机用户名，“password”是该用户密码。

(2) Tskill.

这个命令是用来关掉进程的，其格式：“TSKILL processid | processname [/SERVER:servername] [/ID:sessionid | /A] [/V]”。

参数含义分别为：

processid 要结束的进程的 process ID。

processname 要结束的进程名称。

/SERVER:servername 含有 processID 的服务器（默认值是当前值）。

注
意

使用进程名和/SERVER 时，必须指定/ID 或/A。

/ID:sessionid 结束在指定会话下运行的进程。

/A 结束在所有会话下运行的进程。

/V 显示正在执行的操作信息。

(3) Ntsd.

当使用命令 Tskill 无法结束某进程时，我们就可以尝试命令 Ntsd，其格式为：ntsd -c q -pn {进程名}。

参数含义分别为：

-c 是表示执行 debug 命令。

-q 表示执行结束后退出。

-p 表示后面紧跟着是你要结束的进程对应的 PID。

-pn 表示后面紧跟着是你要结束的进程名。

6.2.4 Windows 系统中常用进程解析小结

作为网管员的我们跟普通用户不同，有些东西普通用户没必要知道的，我们就必须有所了解。比如某计算机出了故障，我们常用的办法是查看进程，如果我们连哪些进程是正常的都不知道，又如何去解决问题呢。所以本节就跟大家一块分享一下常用进程的解析。

(1) 进程文件:taskmgr 或者 taskmgr.exe。

进程名称: the windows task manager

描述: taskmgr.exe 用于 Windows 任务管理器。它显示你系统中正在运行的进程。该程序使用 Ctrl+Alt+Del 组合键打开，这不是纯粹的系统程序，但是如果终止它，可能会导致不可知的问题。

(2) 进程文件:notepad 或者 notepad.exe。

进程名称: notepad

描述: notepad.exe 是 Windows 自带的记事本程序。是 Windows 默认用来打开和编辑文本文件的程序。

(3) 进程文件:wuaucit.exe。

进程名称: autoupdate for windows

描述: wuaucit.exe 是 Windows 自动升级管理程序。该进程会不断在线检测更新。删除该进程将使你无法得到最新更新信息。

(4) 进程文件:alg 或者 alg.exe。

进程名称: application layer gateway service

描述: alg.exe 是微软 Windows 操作系统自带的程序。它用于处理微软 Windows 网络连接共享和网络连接防火墙。这个程序对你系统的正常运行是非常重要的。

(5) 进程文件:timplatform.exe。

进程名称: timplatform

描述: timplatform.exe 是 qq 和 tencent messenger 共同使用的外部应用开发接口管理程序，属于 qq 不可或缺的底层核心模块。如果删除该程序，qq 将丧失与周边功能模块，以及外部应用程序相互调用的功能。

(6) 进程文件:wdfmgr 或者 wdfmgr.exe。

进程名称: windows driver foundation manager

描述: wdfmgr.exe 是微软 microsoftwindowmediaplayer10 播放器的相关程序。该进程用于减少兼容性问题。这不是纯粹的系统程序，但是如果终止它，可能会导致不可预知的问题。

(7) 进程文件:nvsvc32 或者 nvsvc32.exe。

进程名称: nvidiadriverhelperservice

描述: nvsvc32.exe 是 nvidia 显卡相关程序。不要删除此进程，以确保你的图形显示卡的正常运行。

(8) 进程文件:spoolsv 或者 spoolsv.exe。

进程名称: microsoft printer spooler service

描述: spoolsv.exe 用于将 Windows 打印机任务发送给本地打印机。注意 spoolsv.exe 也有可能是 backdoor.ciadoor.b 木马。该木马允许攻击者访问你的计算机，窃取密码和个人数据。

网管天下 网管经验谈

请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 和 servicepackfiles\i386 下面。如果出现在 spoolsv 目录下，则可能是一些 IE 插件的文件，建议使用反间谍进行扫描。

(9) 进程文件:svchost 或者 svchost.exe。

进程名称: microsoft service host process

描述: svchost.exe 是一个属于微软 Windows 操作系统的系统程序，用于执行 dll 文件。这个程序对你系统的正常运行是非常重要的。注意: svchost.exe 也有可能是 w32.welchia.worm 病毒，它利用 windowslsass 漏洞，制造缓冲区溢出，导致你计算机关机。请注意此进程的名字，还有一个病毒是 svch0st.exe，名字中间的是数字 0，而不是英文字母 O。请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 和 servicepackfiles\i386 下面。

(10) 进程文件:frzstate.exe。

进程名称: depfrez

描述: frzstate.exe 是系统还原软件 deep freeze 的相关程序。

(11) 进程文件:ctfmon 或者 ctfmon.exe。

进程名称: alternative user input services

描述: ctfmon.exe 是 microsoft office 产品套装的一部分。它可以选择用户文字输入程序，和微软 office xp 语言条。这不是纯粹的系统程序，但是如果终止它，可能会导致不可知的问题。

(12) 进程文件:rundll32 或者 rundll32.exe。

进程名称: microsoftrundll32

描述: rundll32.exe 用于在内存中运行 dll 文件，它们会在应用程序中被使用。这个程序对你系统的正常运行是非常重要的。注意: rundll32.exe 也可能是 w32.miroot.worm 病毒。该病毒允许攻击者访问你的计算机，窃取密码和个人数据。请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 和 system32\dlldata 下面。

(13) 进程文件:dfservex.exe。

进程名称: dfservex

描述: dfservex.exe 是系统还原软件 deep freeze 的相关程序。

(14) 进程文件:lsass 或者 lsass.exe。

进程名称: local 安全等级作者 ityservice

描述: lsass.exe 是一个关于微软安全机制的系统进程，主要处理一些特殊的安全机制和登录策略。

(15) 进程文件:services 或者 services.exe。

进程名称: windows service controller

描述: services.exe 是微软 Windows 操作系统的一部分。用于管理启动和停止服务。该进程也会处理在计算机启动和关机时运行的服务。这个程序对你系统的正常运行是非常重要的。注意: services 也可能是 w32.randex.r（储存在%systemroot%\system32\目录）和 sober.p（储存在%systemroot%\connection wizard\status\目录）木马。该木马允许攻击者访问你的计算机，窃取密码和个人数据。该进程的安全等级是建议立即删除。

(16) 进程文件:winlogon 或者 winlogon.exe。

进程名称: microsoft windows logon process

描述: winlogon.exe 是 Windows 域登录管理器。它用于处理你登录和退出系统过程。该

操作系统方面 | 6

进程在你系统的作用是非常重要的。注意：winlogon.exe 也可能是 w32.netsky.d@mm 蠕虫病毒。该病毒通过 E-mail 邮件传播，当你打开病毒发送的附件时，即会被感染。该病毒会创建 smtp 引擎在受害者的计算机上，群发邮件进行传播。该病毒允许攻击者访问你的计算机，窃取密码和个人数据。请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 下面。

(17) 进程文件:csrss 或者 csrss.exe。

进程名称：microsoft client/server runtime server subsystem

描述：csrss.exe 是微软客户端/服务端运行时子系统。该进程管理 Windows 图形相关任务。这个程序对你系统的正常运行是非常重要的。注意：csrss.exe 也有可能是 w32.netsky.ab@mm、w32.webus 木马、win32.ladex.a 等病毒创建的。该病毒通过 E-mail 邮件进行传播，当你打开附件时，即被感染。该蠕虫会在受害者计算机上建立 smtp 服务，用以自身传播。该病毒允许攻击者访问你的计算机，窃取木马和个人数据。请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 和 servicepackfiles\i386 下面。

(18) 进程文件:smss 或者 smss.exe。

进程名称：session manager subsystem

描述：smss.exe 是微软 Windows 操作系统的一部分。该进程调用对话管理子系统和负责操作你系统的对话。这个程序对你系统的正常运行是非常重要的。注意：smss.exe 也可能是 win32.ladex.a 木马。该木马允许攻击者访问你的计算机，窃取密码和个人数据。请注意此进程所在的文件夹，正常的进程应该是在 Windows 的 system32 和 servicepackfiles\i386 下面。

(19) 进程文件:system 或 system process。

进程名称：system process

描述：system process 是 Windows 页面内存管理进程，拥有 0 级优先。

(20) 进程文件:system idle 或者 system idle。

进程名称：system idle process

描述：systemidle 不是一个系统进程，用于显示剩余可用的 CPU 资源。

6.2.5 | 修改应用程序访问权限经验

(1) 限制用户对文件的访问权限。

如果程序所在的磁盘分区文件系统为 NTFS 格式，管理员账户可以利用 NTFS 文件系统提供的文件和文件夹安全选项，控制用户对程序及文件的访问权限。通常情况下，一个应用程序安装到系统后，本地计算机的所有账户都可以访问并运行该应用程序。如果取消分配给指定用户对该应用程序或文件夹的访问权限，该用户也就失去了运行该应用程序的能力。

例如，要禁止受限用户运行 Outlook Express 应用程序，可以进行如下的操作。

第 1 步，以 administrator 账户登录系统，如果当前系统启用了简单文件共享选项，需要将该选项关闭。具体做法是，在 Windows 浏览器窗口选择“工具”菜单下的“文件夹选项”命令，弹出“文件夹选项”对话框。打开“查看”选项卡，取消“使用简单文件共享”复选框的选择，单击“确定”按钮，如图 6-8 所示。

第 2 步，打开 Program Files 文件夹，选中 Outlook Express 文件夹并单击右键，在弹出的快捷菜单中选择“属性”命令，如图 6-9 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

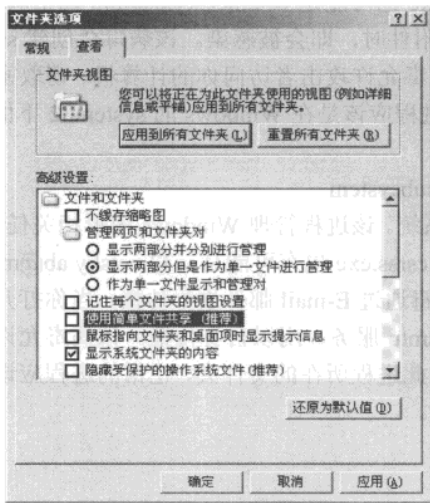


图 6-8 取消“使用简单文件共享”

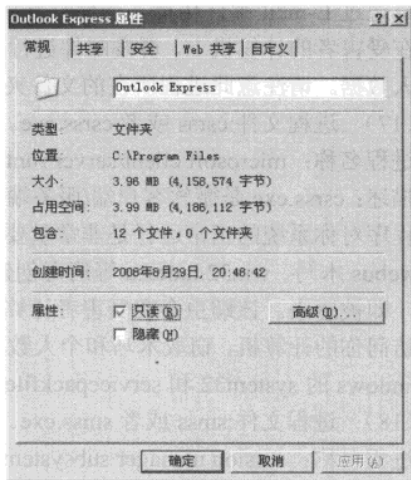


图 6-9 “Outlook Express”属性设置

第 3 步，打开“安全”选项卡，可以看到 Users 组的用户对该文件夹具有读取和运行的权限，单击“高级”按钮，如图 6-10 所示。

第 4 步，取消“从父项继承那些可以应用到子对象的权限项目，包括那些再此明确定义的项目”复选框的选择，在弹出的提示信息对话框，单击“复制”按钮，如图 6-11 所示。此时可以看到用户所具有的权限改为不继承的，如图 6-12 所示。

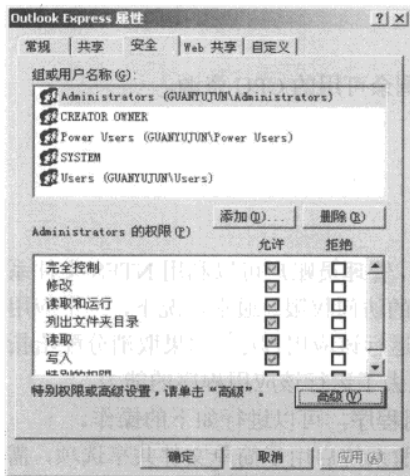


图 6-10 设置高级权限

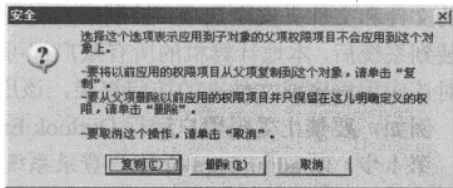


图 6-11 将以前应用的权限复制到这个对象

第 5 步，单击“确定”按钮，返回属性窗口，在“组或用户名称”列表框中，选择 Users 项目，单击“删除”按钮，单击“确定”按钮，完成权限的设置，如图 6-13 所示。

要取消指定用户对文件或程序的访问限制，需要为文件或文件夹添加指定的用户或组，并赋予相应的访问权限。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

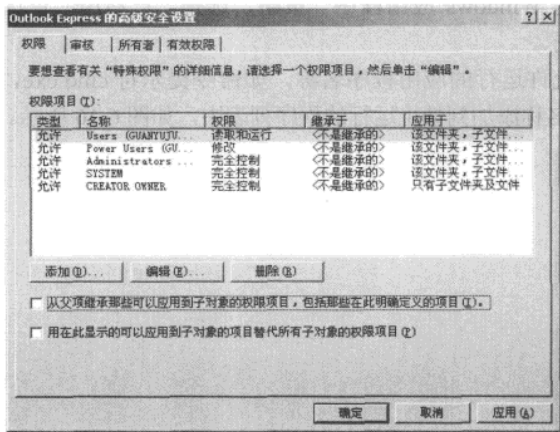


图 6-12 权限改为不继承

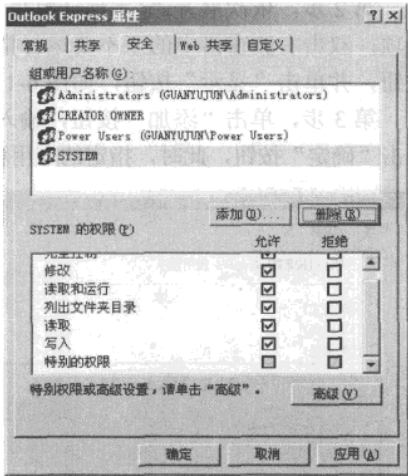


图 6-13 完成权限设置

这种方法允许管理员针对每个用户来限制他访问和运行指定的应用程序的权限。但是需要一个非常重要的前提，那就是要求应用程序所在的分区格式为 NTFS，否则，一切都无从谈起。

对于 FAT/FAT32 格式的分区，不能应用文件及文件夹的安全选项，我们可以通过设置计算机的策略来禁止运行指定的应用程序。

(2) 启用“不要运行指定的 Windows 应用程序”策略。

在组策略中有一条名为“不要运行指定的 Windows 应用程序”策略，通过启用该策略并添加相应的应用程序，就可以限制用户运行这些应用程序。设置方法如下：

第 1 步，在“开始”→“运行”处执行 gpedit.msc 命令，启动组策略编辑器，如图 6-14 所示。或者运行 mmc 命令启动控制台，并将“组策略”管理单元加载到控制台中。

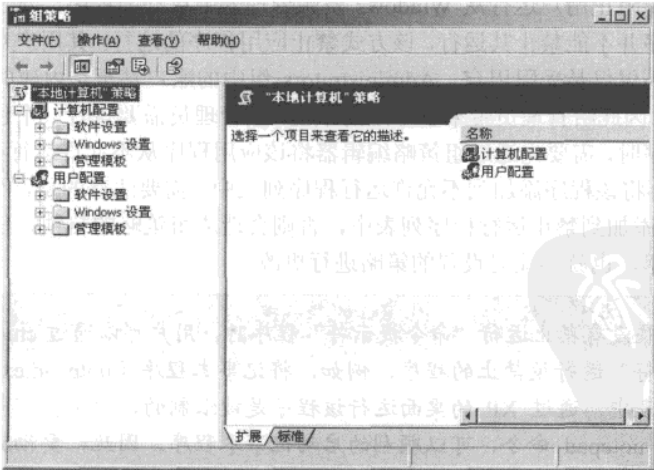


图 6-14 组策略编辑窗口

网管天下 网管经验谈

第2步，依次展开“‘本地计算机’策略”→“用户配置”→“管理模板”，选择“系统”选项，双击右侧窗格中的“不要运行指定的 Windows 应用程序”策略，选择“已启用”单选按钮，并单击“显示”按钮，如图 6-15 所示。

第3步，单击“添加”按钮，输入不允许运行的应用程序名称，如命令提示符 `cmd.exe`，单击“确定”按钮，此时，指定的应用程序名称添加到禁止运行的程序列表中，如图 6-16 所示。

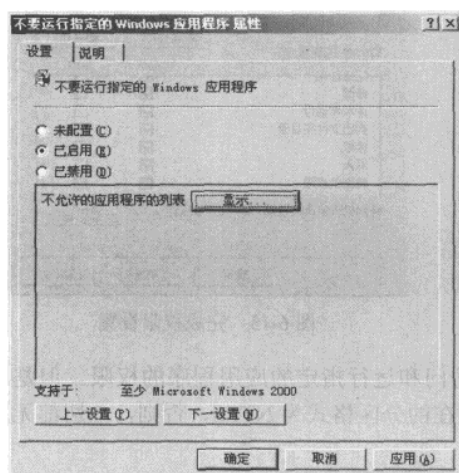


图 6-15 设置“不运行指定的应用程序”

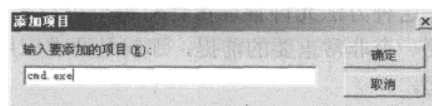


图 6-16 添加项目

第4步，单击“确定”按钮，返回组策略编辑器，单击“确定”按钮，完成设置。

当用户试图运行包含在不允许运行程序列表中的应用程序时，系统会提示警告信息。把不允许运行的应用程序复制到其他的目录和分区中，仍然是不能运行的。要恢复指定的受限程序的运行能力，可以将“不要运行指定的 Windows 应用程序”策略设置为“未配置”或“已禁用”，又或者将指定的应用程序从不允许运行列表中删除（这要求删除后列表不会成为空白的）。

这种方式只能阻止用户运行从 Windows 资源管理器中启动的程序，对于由系统过程或其他过程启动的程序并不能禁止其运行。该方式禁止应用程序的运行，其用户对象的作用范围是所有的用户，而不仅仅是受限用户。Administrators 组中的账户甚至是内建的 administrator 账户都将受到限制，因此给管理员带来了一定的不便。当管理员需要执行一个包含在不允许运行列表中的应用程序时，需要先通过组策略编辑器将该应用程序从不允许运行列表中删除，在程序运行完成后，再将该程序添加到不允许运行程序列表中。需要注意的是，不要将组策略编辑器（gpedit.msc）添加到禁止运行程序列表中，否则会造成组策略的自锁，任何用户都将不能启动组策略编辑器，也就不能对设置的策略进行更改。

提示

如果没有禁止运行“命令提示符”程序时，用户可以通过 `cmd` 命令从“命令提示符”运行被禁止的程序，例如，将记事本程序（`notepad.exe`）添加到不运行列表中，通过 XP 的桌面运行该程序是被限制的，但是在“命令提示符”下运行 `notepad` 命令，可以顺利的启动记事本程序。因此，要彻底的禁止某个程序的运行，首先要将 `cmd.exe` 添加到不允许运行列表中。

(3) 设置软件限制策略。

软件限制策略是本地安全策略的一个组成部分，管理员通过设置该策略对文件和程序进行标识，将它们分为可信任和不可信任两种，通过赋予相应的安全级别来实现对程序运行的控制。这个措施对于解决未知代码和不可信任代码的可控制运行问题非常有效。软件设置策略使用两个方面的设置对程序进行限制，安全级别和其他规则。

安全级别分为“不允许的”和“不受限制的”两种。其中，“不允许的”将禁止程序的运行，不论用户的权限如何；“不受限制的”允许登录用户使用他所拥有的权限来运行程序。

其他规则，即由管理员通过制定规则对指定的一批或一个文件和程序进行标识，并赋予“不允许的”或“不受限制的”安全级别。在这个部分中，管理员可以制定 4 种类型的规则，按照优先级分别是：散列规则、证书规则、路径规则和 Internet 区域规则，这些规则将对文件的访问和程序的运行提供最大限度的授权级别。

1. 软件限制策略的设置

(1) 访问软件限制策略。

作为本地安全策略的一部分，软件限制策略同时也包含在组策略中，这些策略的设置必须以 administrator 账户或 Administrators 组成员的身份登录系统。软件限制策略的访问方式有两种：

第 1 步，在“开始”中的“运行”处运行 secpol.msc，启动本地安全策略编辑器，在“安全设置”下可以看到“软件限制策略”项目，如图 6-17 所示。

第 2 步，在“开始”中的“运行”处运行 gpedit.msc，启动组策略编辑器，在“计算机配置”“Windows 设置”“安全设置”下可以看到“软件限制策略”，如图 6-18 所示。

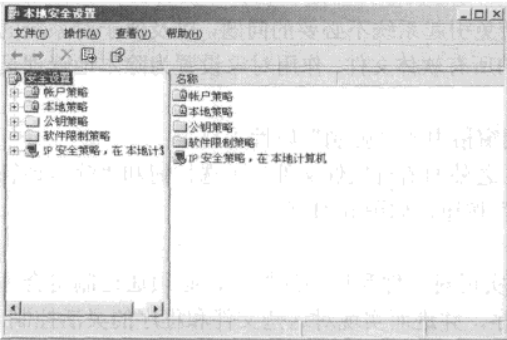


图 6-17 本地安全策略

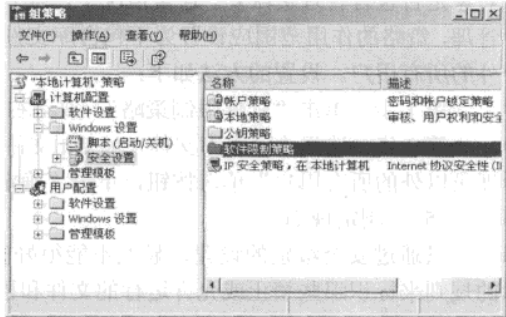


图 6-18 组策略

(2) 新建软件限制策略。

首次打开“软件限制策略”时，该项目是空的。策略需要由管理员手动添加。方法是单击“软件限制策略”使其处于选中状态，选择编辑器窗口“操作”菜单下的“新建一个策略”项目，此时可以看到“软件限制策略”下增加了“安全级别”和“其他规则”及 3 条属性，如图 6-19 所示。一旦执行了新建策略操作后，就不能再次执行该操作，并且这个策略也不能删除。

网管天下 网管经验谈

（3）设置默认的安全级别。

新建软件限制策略后，策略的默认安全级别为“不受限的”，如果要更改默认的安全级别，需要在“安全级别”中进行设置，方法如下。

第1步，打开“安全级别”，在右侧窗格中，可以看到有两条设置，其中图标中带有有一个小对号的设置为默认设置，如图 6-20 所示。

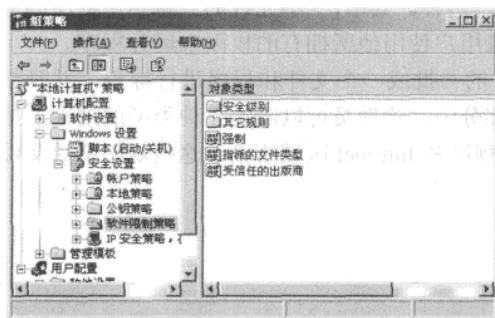


图 6-19 软件设置策略

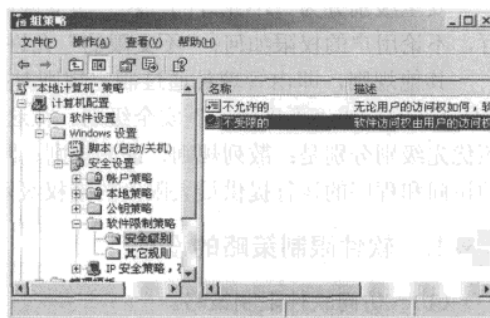


图 6-20 软件默认访问权限

第2步，选择不是默认值的那条设置，单击右键，在弹出的快捷菜单选择“设置为默认”选项。当设置“不允许的”为默认值时，系统会显示一个提示信息对话框，单击“确定”按钮即可。

该步骤也可以双击非默认的设置，在弹出的属性窗口中，单击“设为默认值”按钮。

（4）设置策略的作用范围和对象。

通过策略的“强制”属性，可以设置策略应用的软件文件是否包含库文件，以及作用的对象是否包含管理员账户。通常情况下，为了避免引起系统不必要的问题，以及便于对系统的管理，策略的作用范围应设置为不包含库文件的所有软件文件，作用对象设置为除本地管理员外的所有用户。设置的方法如下：

第1步，单击“软件限制策略”，双击右侧窗格中的“强制”属性项目。

第2步，选择“除去库文件（如 DLL 文件）之外的所有软件文件”单选按钮和“除本地管理员以外的所有用户”单选按钮，单击“确定”按钮，如图 6-21 所示。

（5）制定规则。

只通过安全级别的设置，显然不能很好的实现对文件和程序的控制，必须通过制定合理的规则来标识那些禁止或允许运行的文件和程序，并进而实现对这些文件和程序的灵活控制。上文中提到可制定规则的类型有 4 种：散列规则、证书规则、路径规则和 Internet 区域规则。它们标识文件和制定规则的方法如下：

散列规则：利用散列算法计算出指定文件的散列，这个散列是唯一标识该文件的一系列定长字节。制定了散列规则后，用户访问或运行文件时，软件限制策略会根据文件的散列及安全级别来允许或阻止对该文件进行访问或运行。当文件移动或重命名时，不会影响文件的散列，软件限制策略对该文件依然有效。制定方法如下：

第1步，选择“软件限制策略”下的“其他规则”，在“其他规则”上单击右键，或在右侧窗格的空白区域单击右键，在弹出的快捷菜单中选择“新散列规则”选项，如图 6-22 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

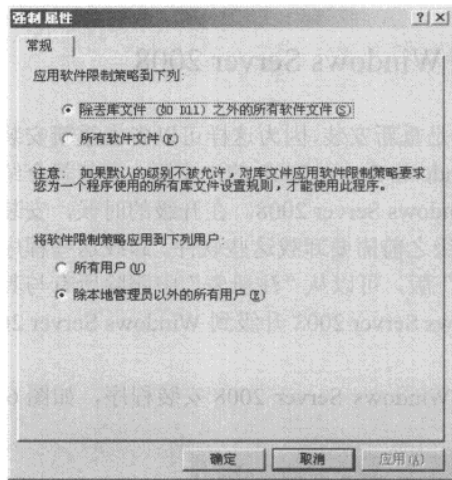


图 6-21 强制属性

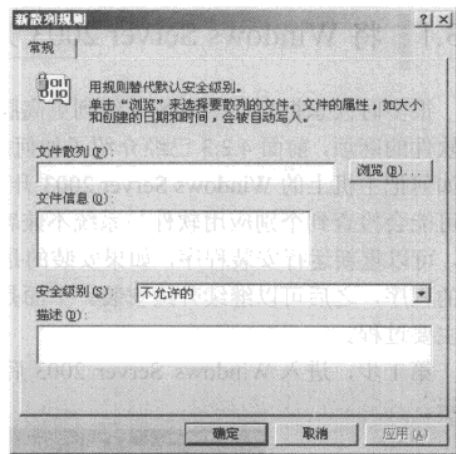


图 6-22 新散列规则

第 2 步，单击“浏览”按钮，指定要标识的文件或程序，例如 ip 查询器.exe，确认后，在文件散列中可以看到计算出来的散列，在“安全级别”中选择“不允许的”或“不受限的”，如图 6-23 所示。单击“确定”按钮，在“其他规则”中可以看到新增了一条类型为散列的规则。



图 6-23 添加指定程序

证书规则：利用与文件或程序相关联的签名证书进行标识。证书规则需要的证书可以是自签名的、由证书颁发机构（CA）颁发或是由 Windows 2003 公钥机构发布的。

6.3 服务器操作系统使用方面的经验

对于服务器操作系统来说应该是所有网管员所熟悉的，所以本节不做过多的赘述。本节只对个人认为相对新的小经验做一些介绍。如何将 Windows Server 2003 升级到 Windows Server 2008、Windows Server 2008 标准证书的使用，以及 Windows Server 2008 新增的功能——Server Core 的安装和配置做一些介绍。

6.3.1 将 Windows Server 2003 升级到 Windows Server 2008

很多时候想把自己的系统升级到更高版本而不是重新安装，因为这样可以省去重新安装应用软件的麻烦，前面 4.2.3 已经介绍了如何制作 Windows Server 2008 的中文版，本节就介绍一下如何把主机上的 Windows Server 2003 升级到 Windows Server 2008。在升级的时候，安装程序可能会检查到个别应用软件与系统不兼容，在升级之前需要卸载这些软件。卸载这些程序之后，可以重新运行安装程序，如果安装的是“绿色”版，可以从“注册表”中删除所有与其相关的程序，之后可以继续升级安装。下面是 Windows Server 2003 升级到 Windows Server 2008 的主要过程。

第 1 步，进入 Windows Server 2003 后，运行 Windows Server 2008 安装程序，如图 6-24 所示。

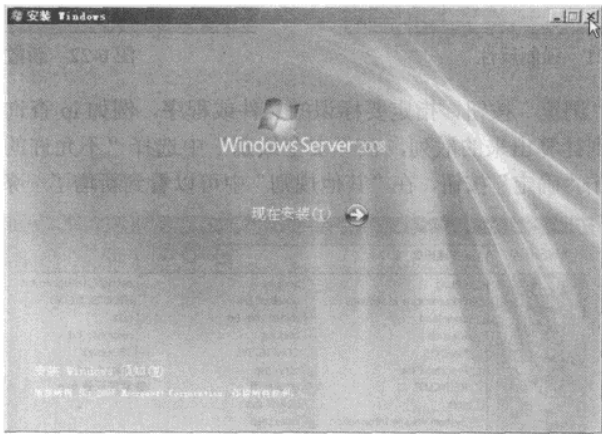


图 6-24 安装

第 2 步，单击“不获取最新安装更新”链接，如图 6-25 所示。

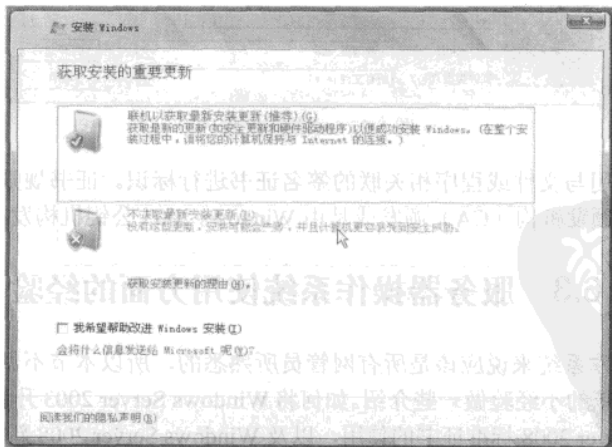


图 6-25 不获取安装更新

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

操作系统方面 | 6

第 3 步，选择“Windows Server 2008 EnterPrise（Full Installation）”选项，单击“下一步”按钮，如图 6-26 所示。

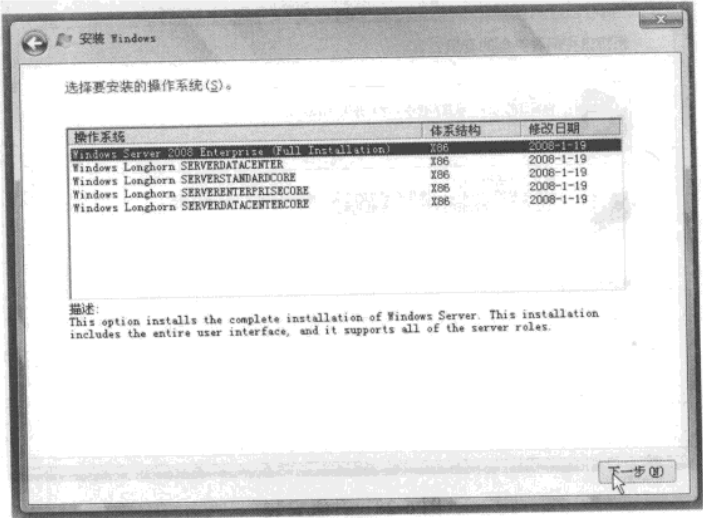


图 6-26 选择需要的版本

第 4 步，选择“我接受许可条款”复选框，单击“下一步”按钮，如图 6-27 所示。

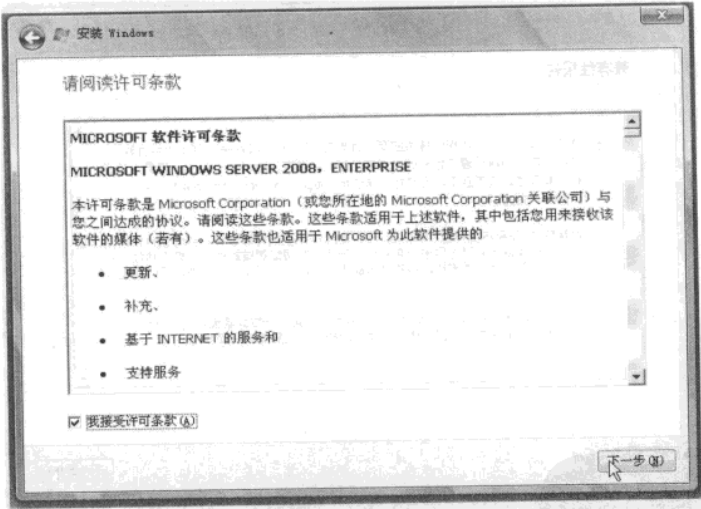


图 6-27 接受许可协议

说·明

使用自己定制的“中文版”，在使用光盘安装的时候，许可协议是“英文”的，而在 Windows 中安装的时候，显示的是全中文的。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 5 步，选择“升级”安装，如图 6-28 所示。



图 6-28 升级安装

第 6 步，进入“兼容性报告”页面，如果检查没问题，会出现“下一步”按钮，如果有问题，出现“关闭”按钮，如图 6-29 所示。

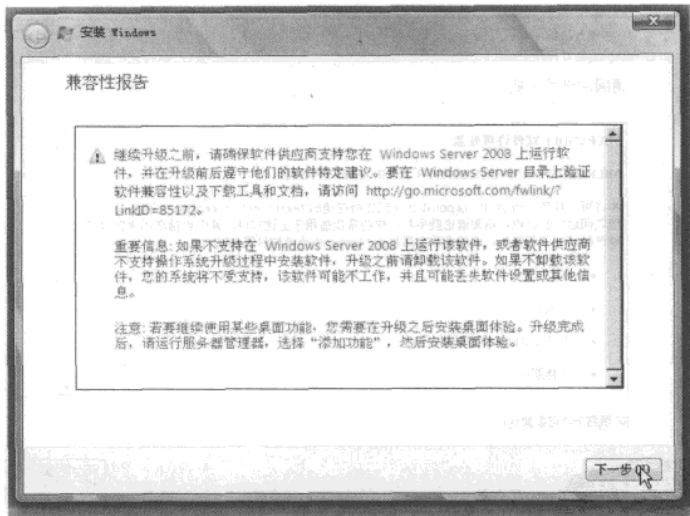


图 6-29 兼容性报告

第 7 步，单击“下一步”按钮，开始升级 Windows，如图 6-30 所示。

这一步大约需要几分钟的时间，完成之后会开始第一次重启。接下来跟安装 2008 的操作一样还会有两次重启才能完成安装，本节就不再赘述。

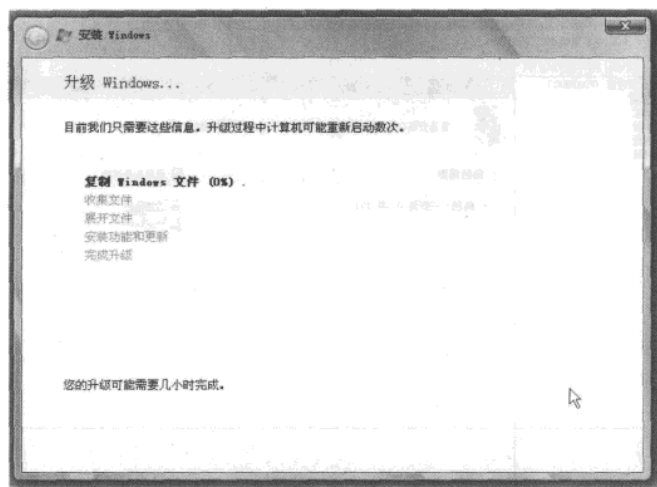


图 6-30 开始升级

6.3.2 | Windows Server 2008 标准证书使用经验

现在很多单位的服务器用的都是 Windows Server 2003，而 Windows Server 2008 早在 2008 年 4 月份就已经发布了正式版。想必有些高调的网管员就想把单位的 Windows Server 2003 丢掉了。然而原来的服务器都已配置好，而且使用很顺利，在升级的过程中和最初的使用过程中会遇到什么样的问题，这些是网管员所必须考虑的。本节就升级证书服务器为案例来介绍一下 Windows Server 2008 的一些证书使用经验。

先将 Windows Server 2003 升级到 2008，再测试 Windows Server 2008 中的“标准 CA”与 Windows Server 2003 提供的“标准 CA”的区别，看是否可以升级。为了避免试验过程中造成损失，使用一台 Windows Server 2008 虚拟机来试验。先安装证书服务，并申请“用户证书”、“计算机证书”，看是否同 Windows Server 2003 时一样。

1. 安装证书服务

第 1 步，在一台 Windows Server 2008 虚拟机中（未安装 IIS、未升级到 AD，其他任何服务器都没有安装），进入“服务器管理器”，定位到“角色”，在右侧窗格单击“添加角色”链接，如图 6-31 所示。

第 2 步，在“选择服务器角色”页中，选中“Active Directory 证书服务”，如图 6-32 所示。

说明 名称叫“Active Directory 证书服务”，并不表示这一定需要 Active Directory 的支持。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

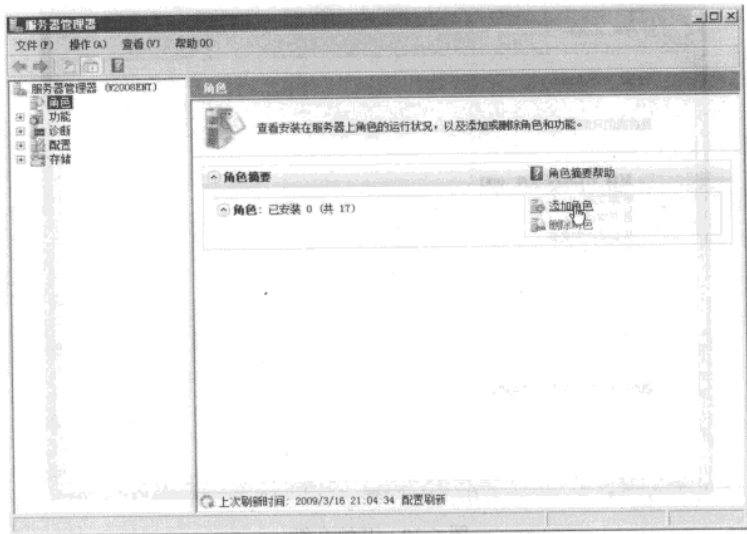


图 6-31 添加角色

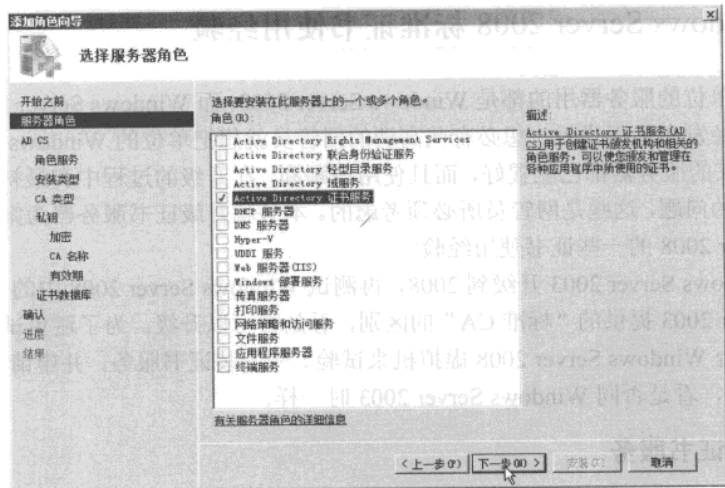


图 6-32 证书服务

第 3 步，在“选择角色服务”页中，添加“证书颁发机构”、“证书颁发机构 Web 注册”、“联机响应程序”，在选择“证书颁发机构 Web 注册”时，会弹出“添加角色向导”对话框，单击“添加必需的角色服务”按钮，即可自动添加所需要的 IIS 服务，如图 6-33 所示。

第 4 步，在“指定安装类型”页中，选择“独立”单选按钮，这就是表示要安装“标准 CA 证书”服务器了，如图 6-34 所示。

第 5 步，在“指定 CA 类型”页中，选择“根”单选按钮，如图 6-35 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

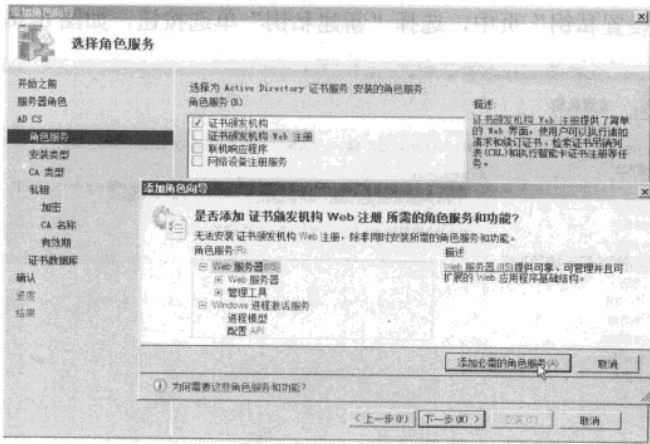


图 6-33 添加角色

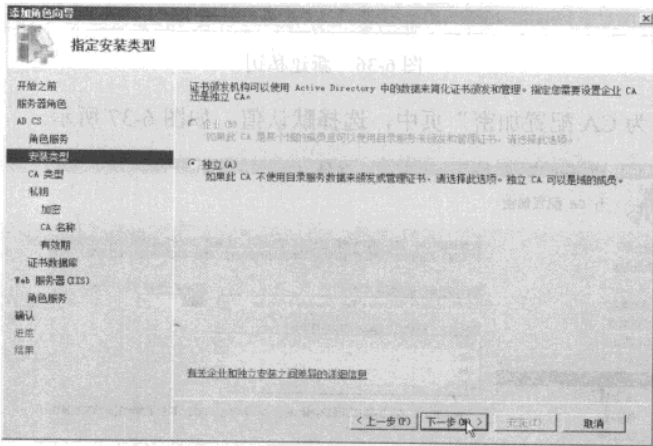


图 6-34 添加标准证书服务器

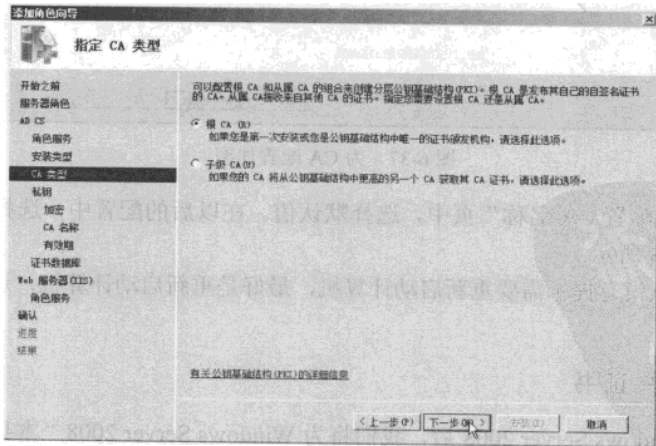


图 6-35 根 CA

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 6 步，在“设置私钥”页中，选择“新建私钥”单选按钮，如图 6-36 所示。

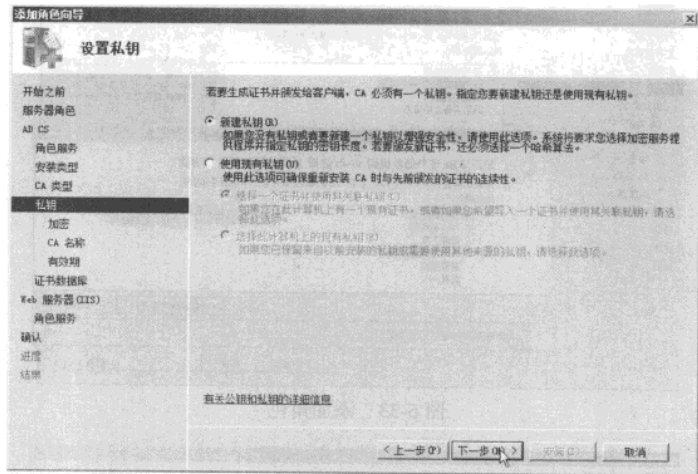


图 6-36 新建私钥

第 7 步，在“为 CA 配置加密”页中，选择默认值，如图 6-37 所示。

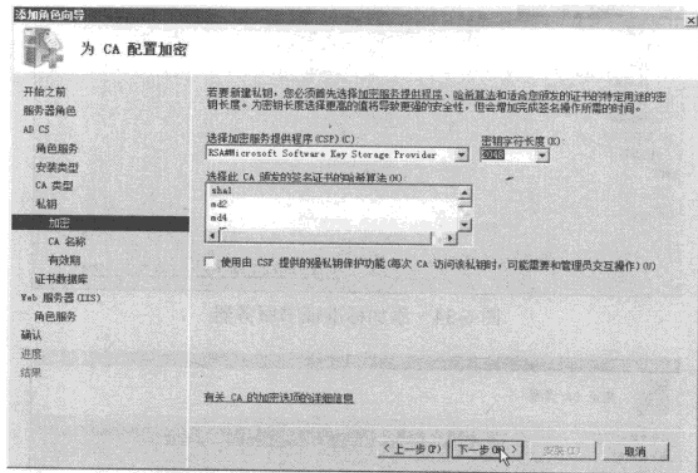


图 6-37 为 CA 配置加密

第 8 步，在“配置 CA 名称”页中，选择默认值。在以后的配置中，选择默认值，直接安装完成，如图 6-38 所示。

第 9 步，虽然没有提示需要重新启动计算机，最好是重新启动计算机，让设置生效，如图 6-39 所示。

2. 申请用户证书

再次进入 Windows Server 2008 后，我们将为 Windows Server 2008 “本身”申请一个 Web 服务器证书。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

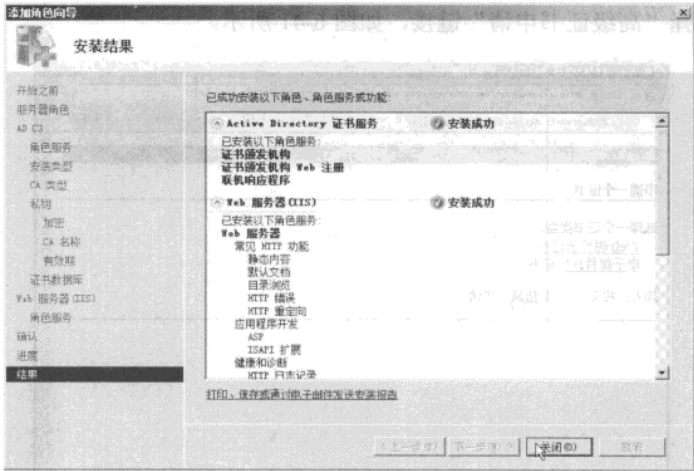


图 6-38 安装完成



图 6-39 重新启动计算机

第 1 步，打开 IE 浏览器，输入 <http://localhost/certsrv/>，如图 6-40 所示。然后单击“申请证书”链接。

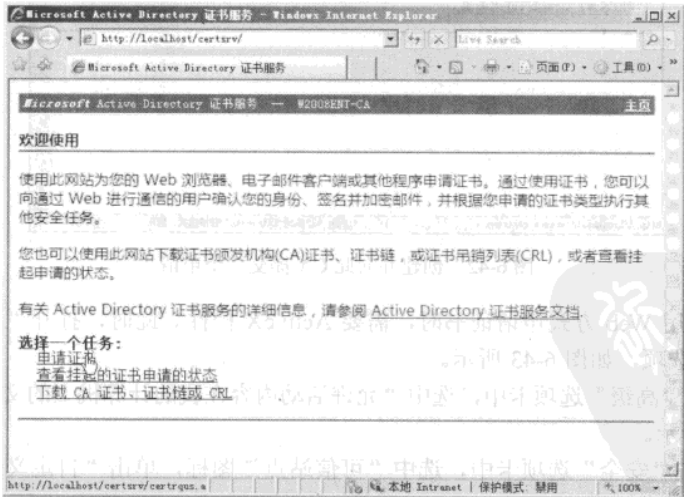


图 6-40 申请证书

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 2 步，选择“高级证书申请”链接，如图 6-41 所示。

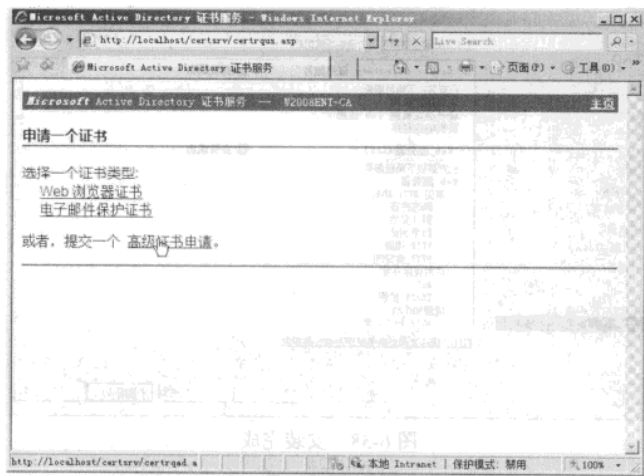


图 6-41 高级证书申请

第 3 步，在“高级证书申请”页中，单击“创建并向此 CA 提交一个申请”链接，如图 6-42 所示。

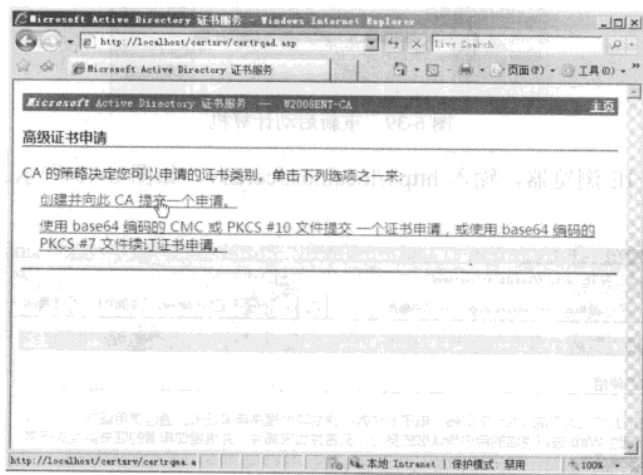


图 6-42 创建并向此 CA 提交一个申请

第 4 步，使用 Web 方式申请证书时，需要 ActiveX 控件。此时，打开“工具”菜单选择“Internet 选项”选项，如图 6-43 所示。

第 5 步，在“高级”选项卡中，选中“允许活动内容在我的计算机上的文件中运行”复选框，如图 6-44 所示。

第 6 步，在“安全”选项卡中，选中“可信站点”图标，单击“自定义级别”按钮，如图 6-45 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

操作系统方面 | 6



图 6-43 Internet 选项



图 6-44 允许活动内容在计算机上运行

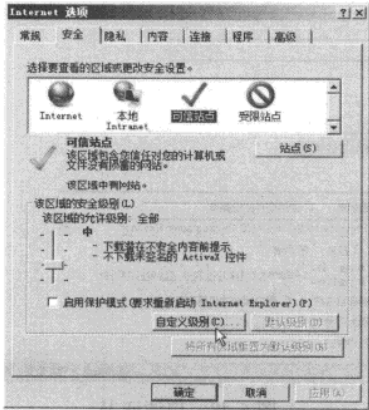


图 6-45 自定义级别

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 7 步，在“安全设置—受信任的站点区域”对话框中，选中“ActiveX 控件自动提示”、“对标记为可安全执行脚本的 ActiveX 控件执行程序”、“下载已签名的 ActiveX 控件”等，如图 6-46 所示。

第 8 步，返回到图 6-45 后，单击“站点”按钮，添加 http://localhost 到可信区域，如图 6-47 所示。



图 6-46 执行 ActiveX 控件

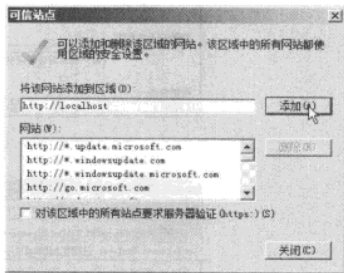


图 6-47 添加当前站点到可信区域

第 9 步，返回到 IE 浏览器后，按 F5 键刷新，可以申请证书。在此，申请证书的名称与计算机名称一致，并在“需要的证书类型”中选择“服务器身份验证证书”选项，并选中“标记密钥为可导出”复选框，如图 6-48 所示。

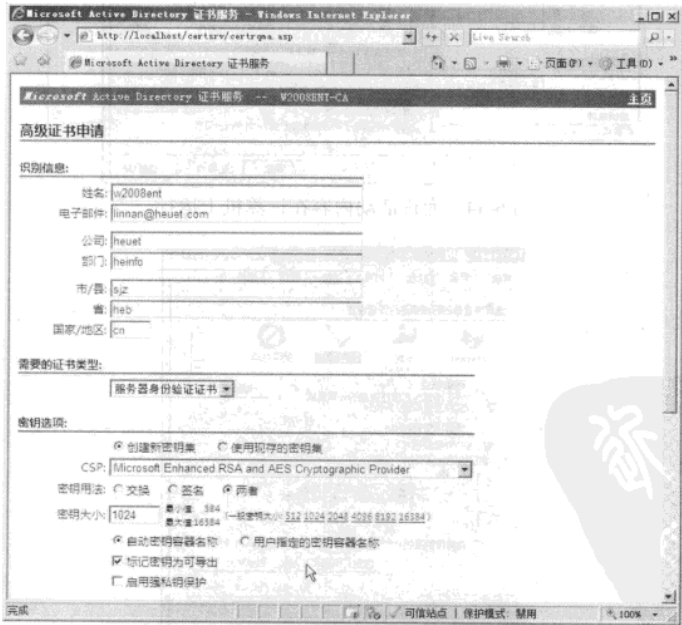


图 6-48 申请证书

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 10 步，提交申请后，提示“证书正在挂起”，如图 6-49 所示。

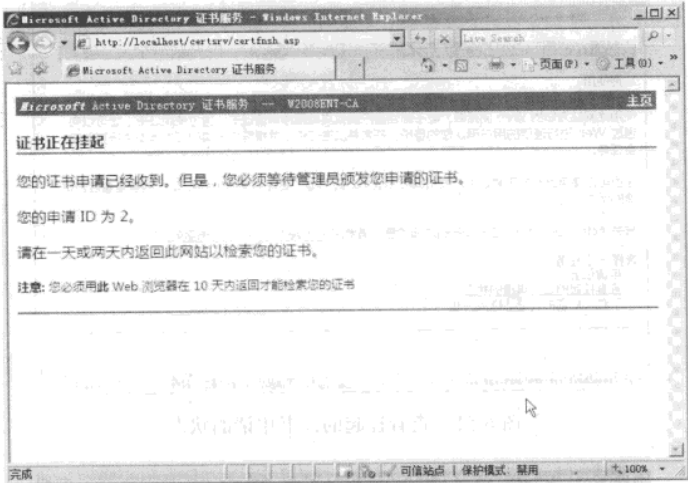


图 6-49 证书申请被挂起

第 11 步，返回到“服务器管理器”窗口，定位到“角色→W2008ENT-CA→挂起的申请”，在右侧，颁发申请的证书，如图 6-50 所示。

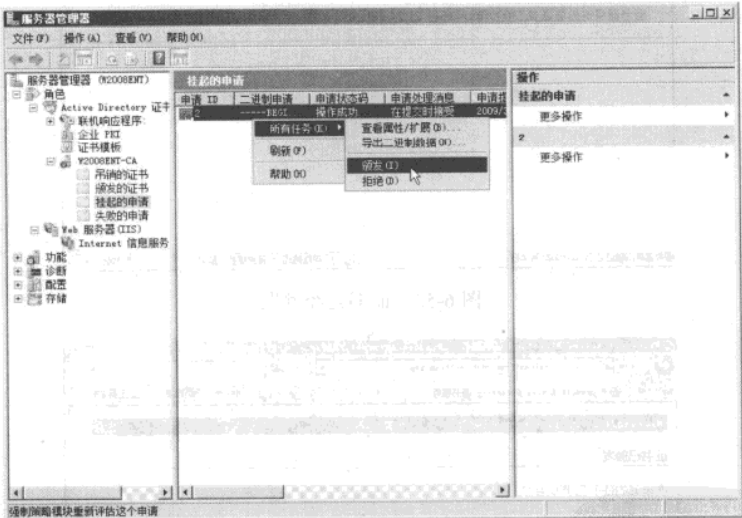


图 6-50 颁发证书

第 12 步，切换到 IE 浏览器，单击“主页”按钮，单击“查看挂起的证书申请的状态”链接，如图 6-51 所示。

第 13 步，可以看到，证书已经被颁发，如图 6-52 所示。

第 14 步，单击“安装此证书”链接，如图 6-53 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

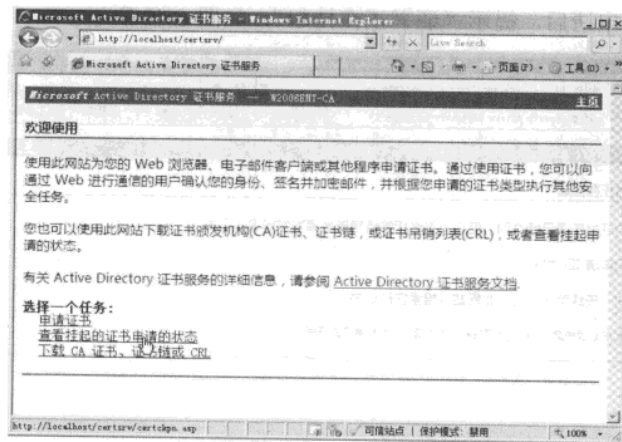


图 6-51 查看挂起的证书申请的状态

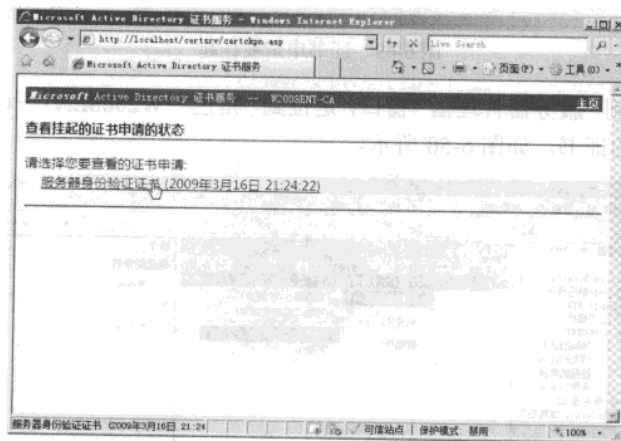


图 6-52 证书已经颁发

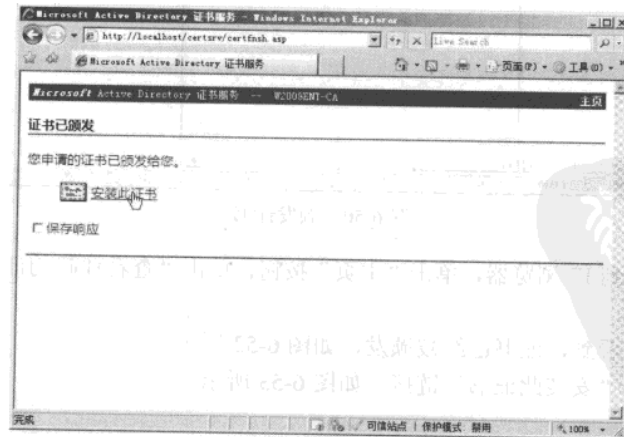


图 6-53 安装证书

3. 证书

由于在 Windows Server 2008 中，不能直接申请“计算机证书”，所以，要想安装计算机证书，必须将上一步申请的证书，从“用户证书”存储中导出，然后再“导入”到计算机存储中，成为“计算机证书”，主要步骤如下。

第 1 步，在 IE 浏览器中，进入“Internet 选项”，在“内容”选项卡中，单击“证书”按钮，如图 6-54 所示。

第 2 步，在“证书”页中的“个人”选项卡中，单击“导出”按钮，如图 6-55 所示。

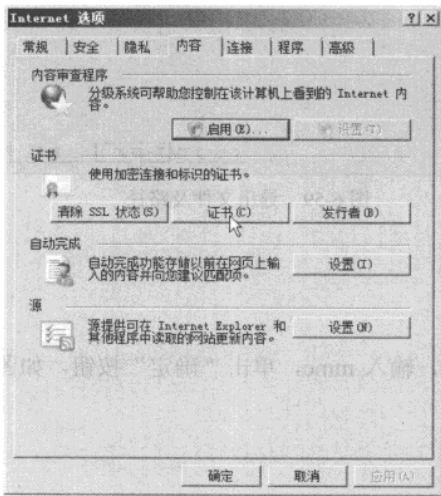


图 6-54 证书

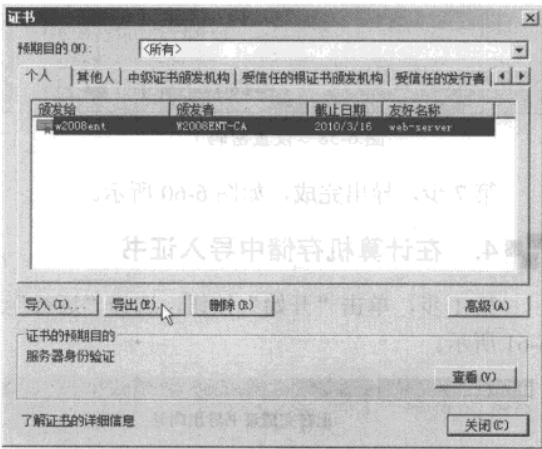


图 6-55 导出证书

第 3 步，在“导出私钥”页中，选中“是，导出私钥”单选按钮，如图 6-56 所示。

第 4 步，在“导出文件格式”页中，选中“如果导出成功，删除密钥”复选框，如图 6-57 所示。

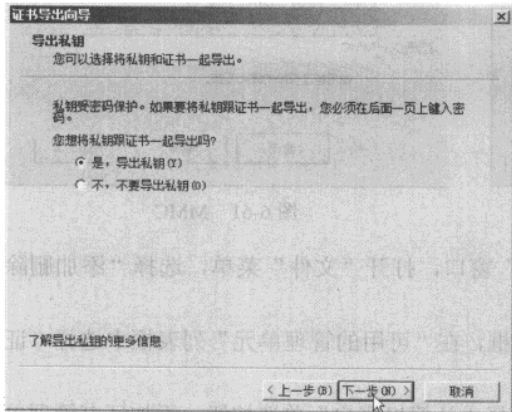


图 6-56 导出私钥

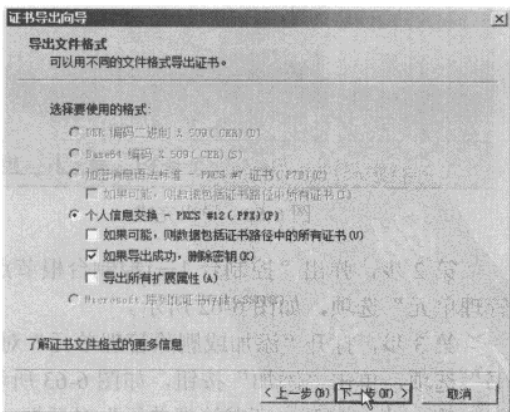


图 6-57 导出后删除密钥

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下

网管经验谈

第 5 步，在“密码”页中，设置密码，如图 6-58 所示。
第 6 步，设置导出文件的名称及路径，如图 6-59 所示。

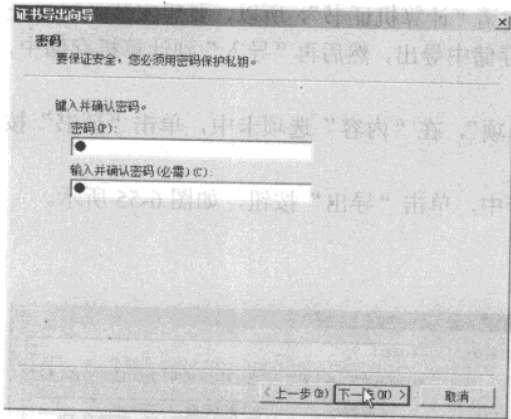


图 6-58 设置密码

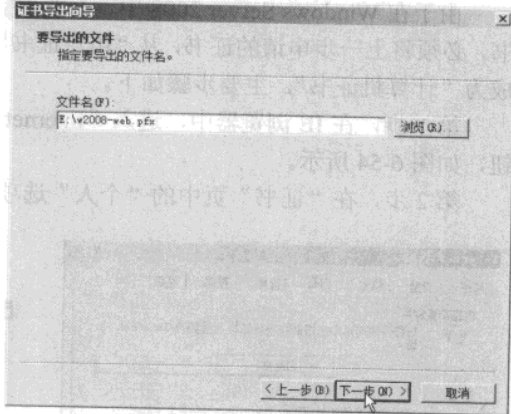


图 6-59 导出文件及路径

第 7 步，导出完成，如图 6-60 所示。

4. 在计算机存储中导入证书

第 1 步，单击“开始”按钮，选择“运行”选项，输入 mmc，单击“确定”按钮，如图 6-61 所示。

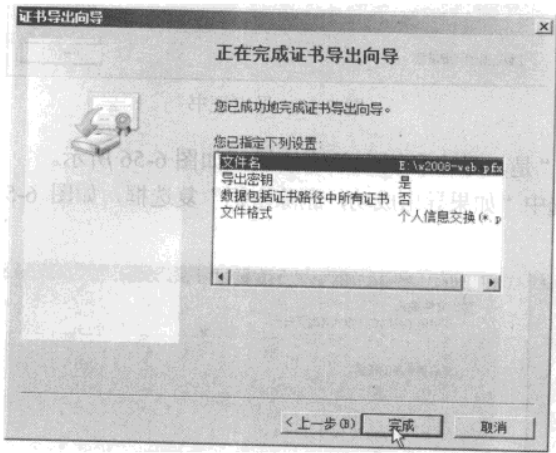


图 6-60 导出完成

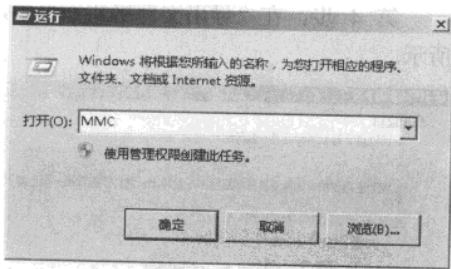


图 6-61 MMC

第 2 步，弹出“控制台 1—[控制台根节点]”窗口，打开“文件”菜单，选择“添加删除管理单元”选项，如图 6-62 所示。

第 3 步，打开“添加或删除管理单元”对话框，在“可用的管理单元”列表框中选择“证书”选项，单击“添加”按钮，如图 6-63 所示。

第 4 步，打开“证书管理单元”对话框，选择“计算机账户”单选按钮，添加证书管理单元，单击“下一步”按钮如图 6-64 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

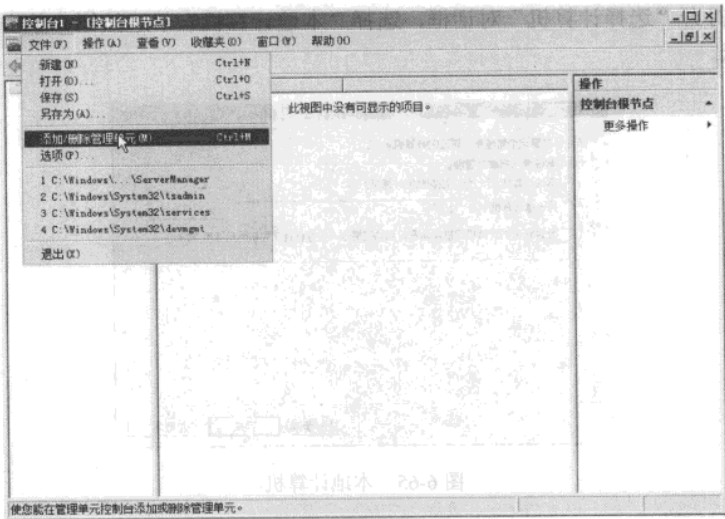


图 6-62 添加管理单元

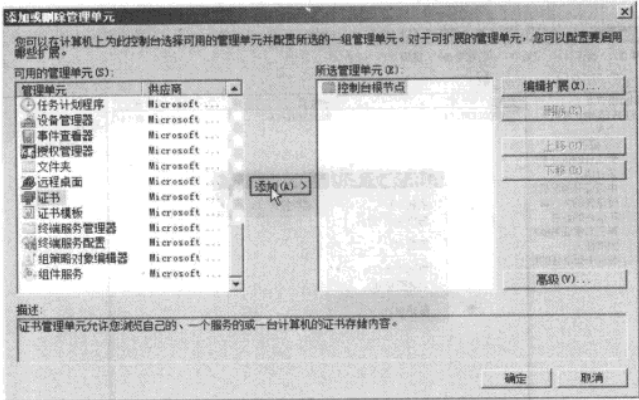


图 6-63 添加证书

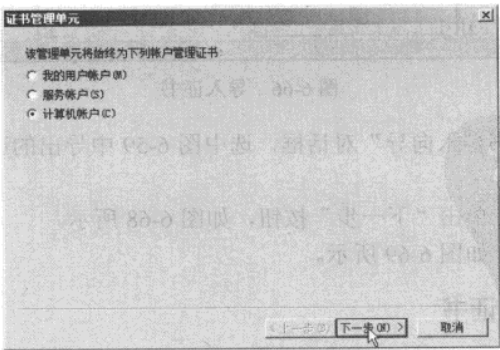


图 6-64 计算机账户

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 5 步，打开“选择计算机”对话框，选择“本地计算机”单选按钮，单击“完成”按钮，如图 6-65 所示。

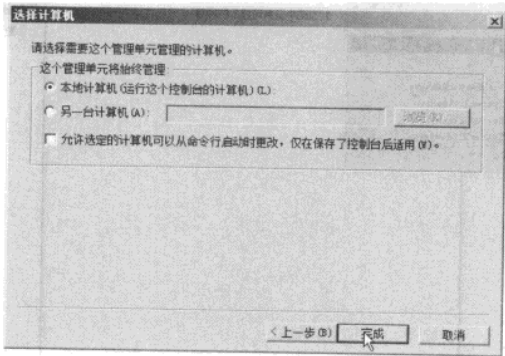


图 6-65 本地计算机

第 6 步，返回到 MMC 管理控制台后，定位到“证书→个人→证书”，导入证书，如图 6-66 所示。

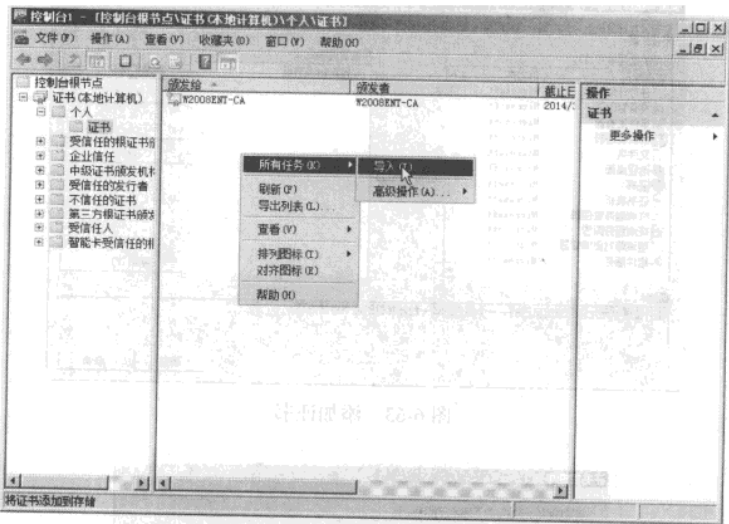


图 6-66 导入证书

第 7 步，打开“证书导入向导”对话框，选中图 6-59 中导出的证书，单击“下一步”按钮如图 6-67 所示。

第 8 步，输入密码，单击“下一步”按钮，如图 6-68 所示。

第 9 步，导入完成，如图 6-69 所示。

5. 在 IIS 中分配证书

返回到“服务器管理器”，定位到“Web 服务器→Internet 信息服务”，在右侧的任务窗格中单击“绑定”链接，如图 6-70 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

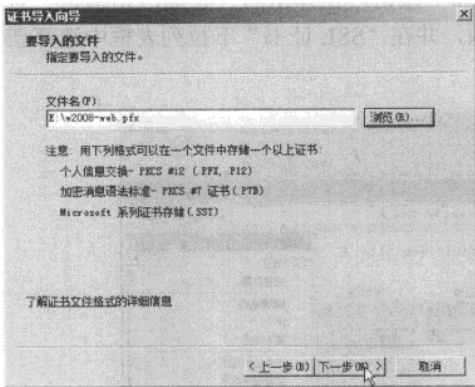


图 6-67 导入证书

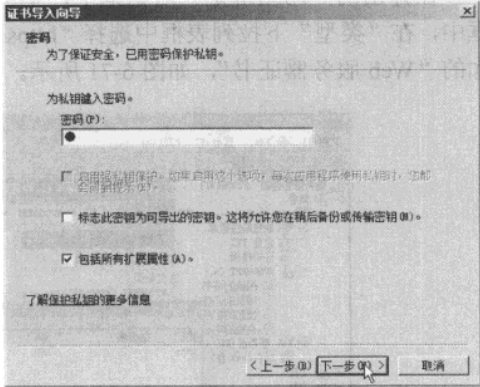


图 6-68 输入密码

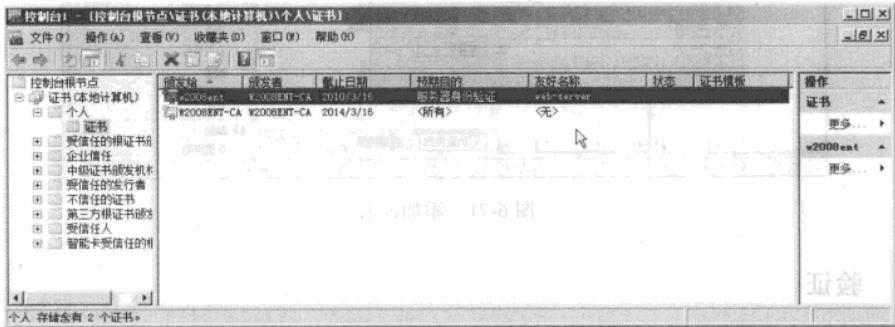


图 6-69 导入证书完成



图 6-70 绑定

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

在弹出的“网站绑定”对话框中，单击“添加”按钮，在弹出的“添加网站绑定”对话框中，在“类型”下拉列表框中选择“https”选项，并在“SSL 证书”下拉列表框中选择新添加的“Web 服务器证书”，如图 6-71 所示。

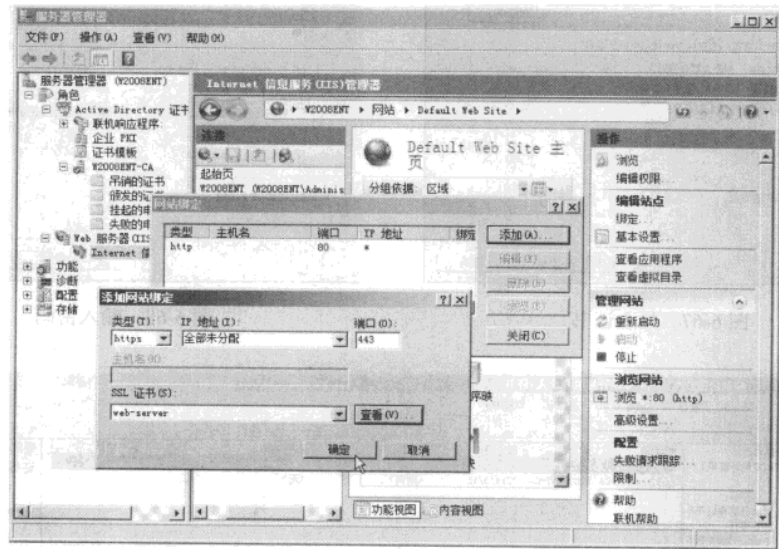


图 6-71 添加证书

6. 验证

返回到 IE 浏览器中，输入 https://w2008ent，此时会打开默认的网站，如图 6-72 所示。



图 6-72 默认站点

输入 https://w2008ent/certsrv，也可以正常浏览，如图 6-73 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

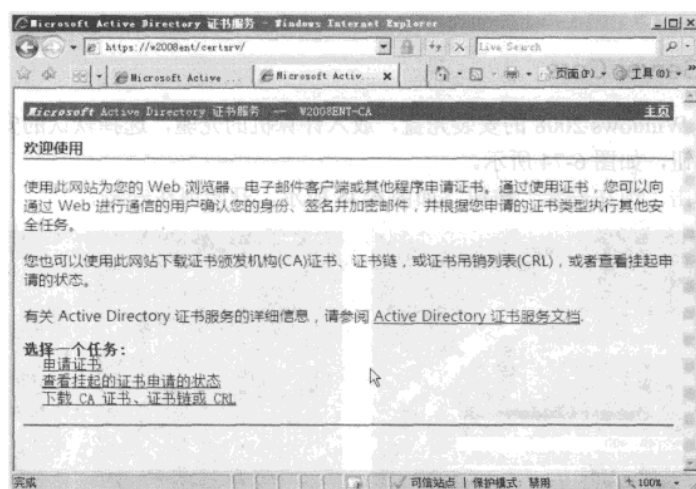


图 6-73 浏览证书申请站点

说·明

经过测试发现，Windows Server 2008 的标准证书服务，是完全可以代替 Windows Server 2003 的证书服务的。另外，Windows 2008 的证书服务中，已经取消了“存储到本地”这一选项，也就是说，不能直接申请“计算机证书”，只能是先将申请的用户证书导出，再导入成“计算机证书”。

6.3.3 体验 Windows2008 新功能——Server Core 的安装和配置

Windows Server 2008 正式发布也一年多了，但是大多数人对 Windows Server 2008 仍然很不熟悉，甚至很多人认为就是比 Windows Server 2003 更强大一点，但是强在哪里就不知道了。其实 Windows Server 2008 确实比 Windows Server 2003 强大，最起码它新增的功能 server Core 就很好。本节就介绍一下 server Core 的安装和配置。

对于 server Core（服务器核心），我们都知道，以前微软的操作系统几乎全部是图形界面，虽然命令功能也很强大，但只要人们一提起微软的操作系统就想起图形界面，就想起会不断的打补丁，是黑客攻击的对象。孰不知，现在微软有意在增强其命令行的操作，而在微软的 2008 的服务器操作系统里多了一个十分重要的角色——Server Core。简单来说就是一个只有字符，几乎没有图形界面的类似 UNIX 或 Linux 的字符操作系统。而在 Server Core 中我们可以实现多种服务或功能，如 DNS、DHCP、WINS、打印服务、文件服务器、NLB 等。微软推出 Server Core 的定位非常清楚，安全稳定的小型专用服务器。如果你的企业有很多分支，你可以在分支机构部署一台 Server Core，并让它扮演 RODC（只读域控制器），这样在一定程度上既保证了分支客户端登录域的速度，同时也保证了安全性。

我们已经有了一个 Windows 2008 的域环境，heuet.com 是域控制器，要求安装一台 Server Core，主机名为 ser-c，IP 地址的设置是 172.21.21.22，DNS 地址是 172.21.21.21，网关是

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

172.21.1.1。

1. 安装 Server Core

第 1 步，把 Windows 2008 的安装光盘，放入计算机的光驱，选择默认的安装环境，再单击“下一步”按钮，如图 6-74 所示。

第 2 步，单击“现在安装”按钮，如图 6-75 所示，开始现在安装。

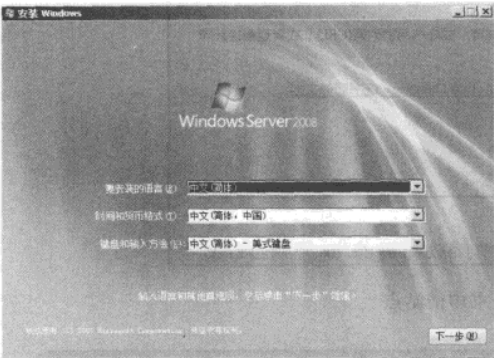
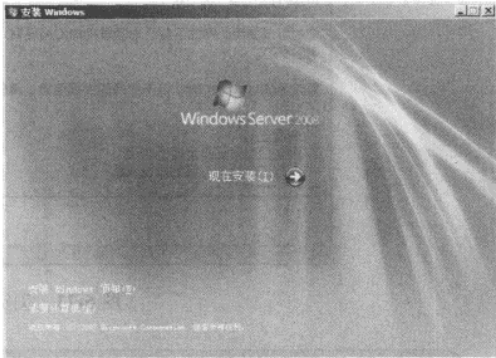


图 6-74 选择安装环境



6-75 现在安装

第 3 步，选择“Windows Server 2008 Standard 服务器核心安装”选项，然后单击“下一步”按钮，如图 6-76 所示。在请“请阅读许可条款”页中，选择“我接受许可条款”复选框，如图 6-77 所示，再单击“下一步”按钮。

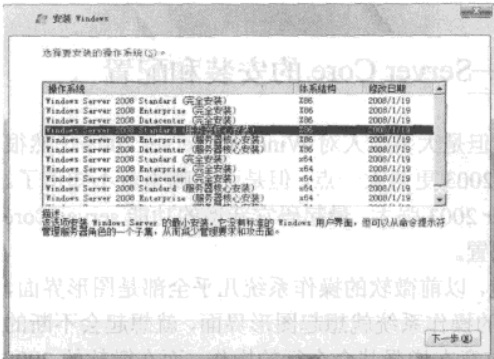


图 6-76 选择安装版本

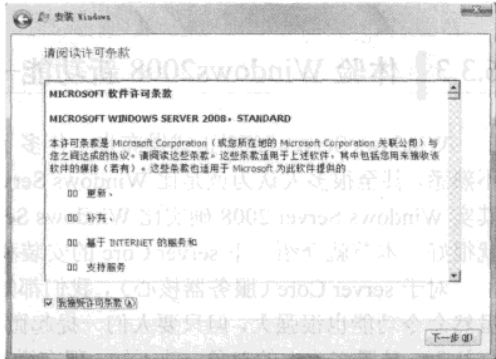


图 6-77 接受许可条款

第 4 步，在“你想进行何种类型的安装？”页中，选择“自定义（高级）”安装，如图 6-78 所示。

第 5 步，在“你想将 Windows 安装在何处？”页中，选择安装磁盘，在这里只有 DISK0，所以就选它，然后单击“下一步”按钮，如图 6-79 所示。

第 6 步，开始复制文件，进行安装过程，这个过程较慢，请耐心等待！跟安装其他系统一样安装过程要重启几次，最后进入登录界面，第一次登录，管理员要改密码，默认是空，取一个复杂密码即可，如 123369pnW 就行了，如图 6-80 所示。登录后的界面对于习惯用 Windows

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的人来说是比较新鲜的，如图 6-81 所示。

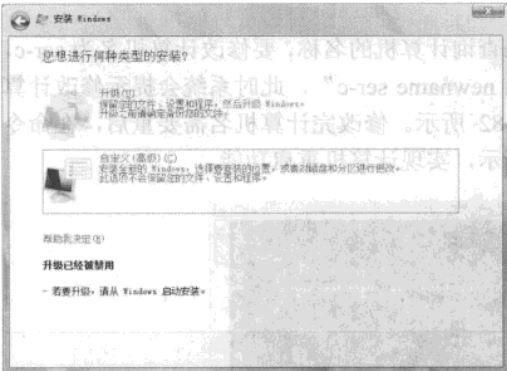


图 6-78 选择“自定义”安装

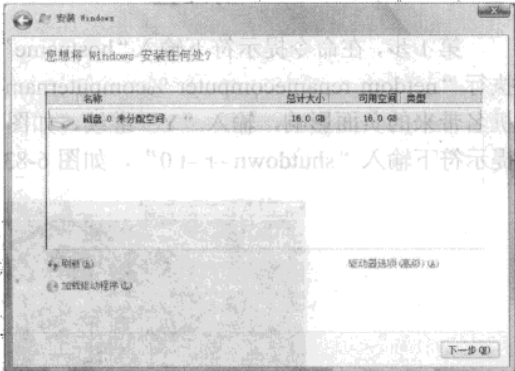


图 6-79 选择安装磁盘

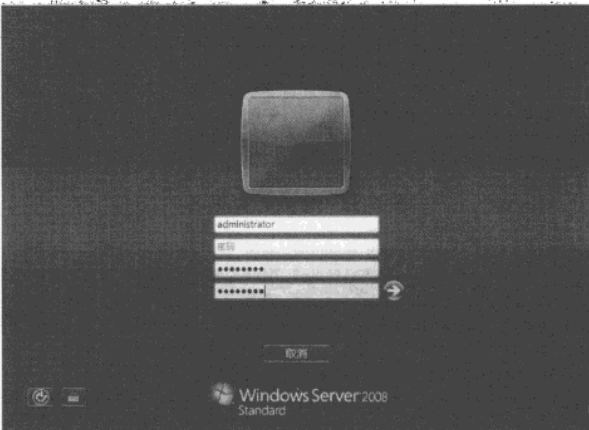


图 6-80 第一次登录 2008

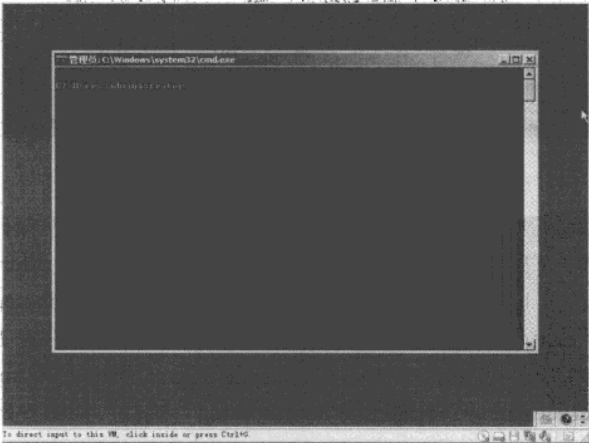


图 6-81 登录 Server Core 界面

2. Server Core 的配置

第 1 步，在命令提示符下输入“hostname”来查询计算机的名称，要修改计算机名为 ser-c，执行“netdom renamecomputer %computername% newname ser-c”，此时系统会提示修改计算机名带来的负面影响，输入“Y”继续，如图 6-82 所示。修改完计算机名需要重启，在命令提示符下输入“shutdown -r -t 0”，如图 6-83 所示，实现计算机重启功能。



图 6-82 修改计算机名



图 6-83 重启计算机

第 2 步，修改完计算机名，重启后就要设置静态的 IP 地址，子网掩码，网关地址及 DNS 等。方法是分别在命令提示符下输入“netsh interface ipv4 set address”本地连接“static 172.21.21.22 255.255.0.0 172.21.1.1”和“netsh interface ipv4 set dnsserver”本地连接“static 172.21.21.21 primary”如图 6-84 所示实现该设置功能。如果企业里存在 DHCP 服务器，也可以在命令提示符下输入“netsh interface ipv4 set address name=“本地连接”source=dhcp”和“netsh interface ipv4 set dnsserver name=“本地连接”source=dhcp”执行，如图 6-85 所示实现自动获取地址的功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

操作系统方面 | 6

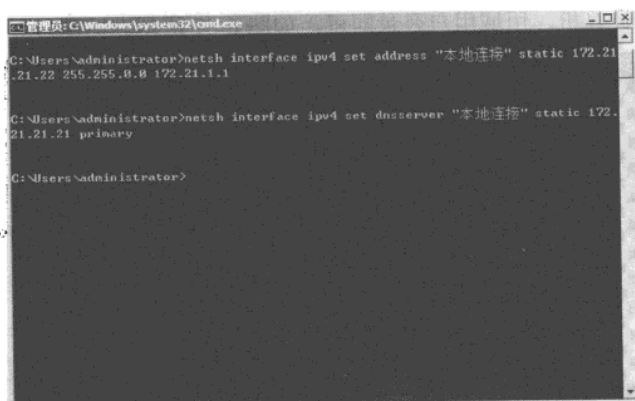


图 6-84 设置 IP，网关和 DNS 等

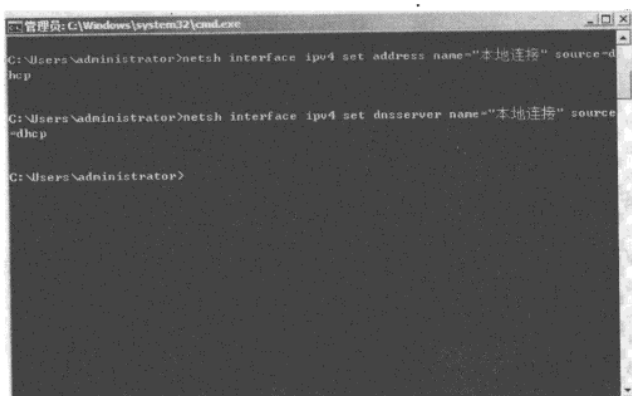


图 6-85 设置自动获取地址

第 3 步，通过执行“netdom Join ser-c \domain:heuet.com /userd:administrator /passwordd:123369pnW”，实现计算机加入到域 heuet.com 的功能，如图 6-86 所示。

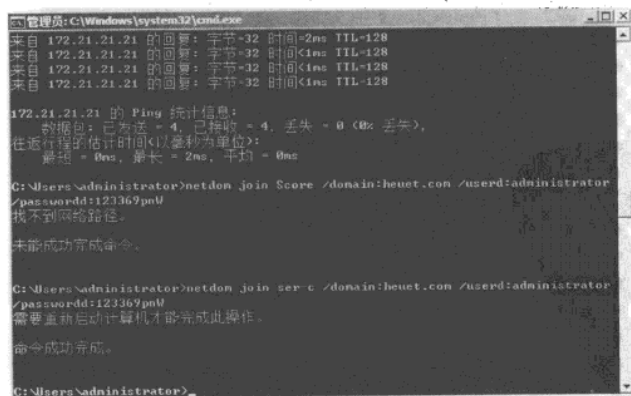


图 6-86 计算机加入域

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 4 步，重启计算机，用域用户登录即可，如图 6-87 所示。

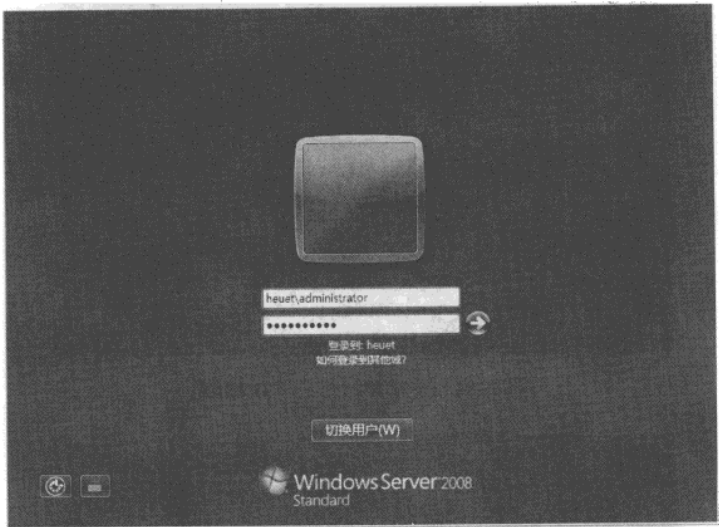


图 6-87 用域用户登录

3. 安装服务器角色

(1) 在一般 Windows Server 2008 环境中，我们可以使用服务器管理员，来新增或移除各项服务器角色或特性套件，而在 Server Core 中，则有专门套件管理的指令。通过执行“oclist”指令实现以树状结构列出所有服务器内的角色及特性等套件，并显示该套件安装与否，如图 6-88 所示（该命令只能在 Server Core 中使用）。



图 6-88 查看服务器角色

(2) 通过执行“ocsetup [套件名称]”命令，实现安装或移除服务器角色与特性套件的功

操作系统方面 | 6

能。如：“ocsetup IIS-WebServerRole”——“IIS 网页服务器”输入时要注意套件名称的大小写，而真正的套件名称就如同 OClist 中列出。当我们执行套件安装后，若指令语法正确，就会回到命令提示列下，而系统会在背景安装指定套件完成后可用 OClist 确认已经安装，但系统不会另外出现任何提示，告知我们套件已经装好，如图 6-89 所示。（此套指令和 OClist 相同，仅有 Server Core 环境才支持。）可将安装指令改为 start /w ocsetup IIS-WebServerRole，start 是执行后面程序，而参数 w 是等待该程序结束，才释出提示光标，好让管理人员掌握安装进度，如图 6-90 所示（一般安装服务或功能时，使用“start /w ocsetup 服务名”即可，但由于服务名等是区分字母大小写的，所以事先先用 oclicst 来查看服务的名字，再进行安装）。

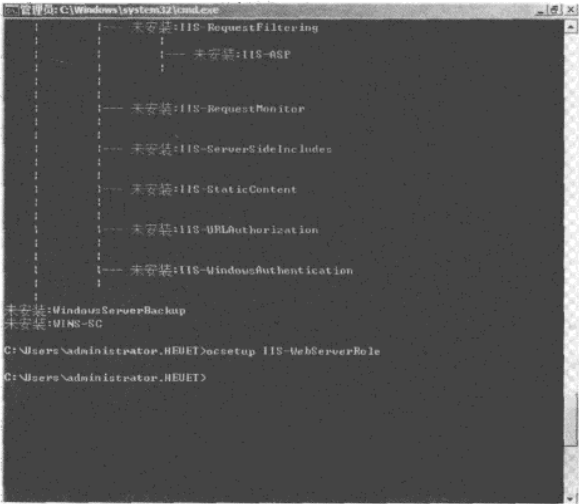


图 6-89 安装 IIS 网页服务器

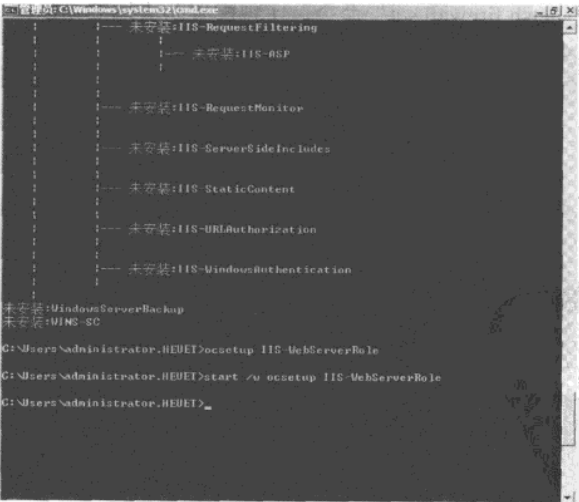


图 6-90 改进后的安装命令

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

(3) 通过执行“oclist”来查看 IIS 网页服务器是否安装成功，如图 6-91 所示。



图 6-91 IIS 已安装

(4) 通过执行“net user administrator *”命令，实现修改管理员密码的功能，如图 6-92 所示（*代表你要设的密码，在这里为 123369pnW）。



图 6-92 设置密码

(5) 通过执行“netsh firewall set”命令，实现配置防火墙的功能，如图 6-93 所示。

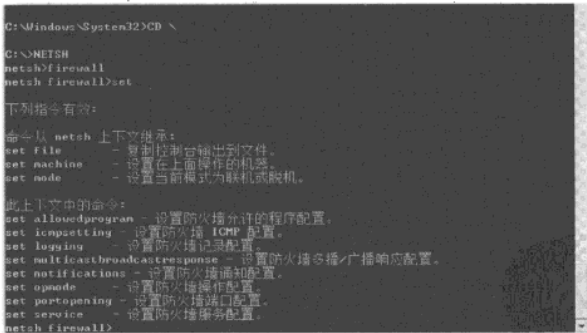


图 6-93 配置防火墙

第 7 章 高可用性应用

部分企业对系统应用要求很高，例如金融行业对系统要求是 99999，如果其中的一台服务器出现故障，不能影响业务的正常运作。提供系统可用性的方法有很多，本章以常见的高可用性为例，说明如何提高系统稳定性，保证业务正常运行。

7.1 磁盘高可用性

磁盘是存储数据的主体。磁盘的损坏不仅将直接导致系统瘫痪和网络服务失败，而且还将导致宝贵的存储数据丢失，所造成的损失往往是难以估量的。为了提高系统的稳定性和数据安全性，服务器通常采用 Raid 卡实现磁盘冗余，既保证了系统和数据的安全，同时又提高了数据的读取速率和数据存储容量。

7.1.1 常见 Raid 类型

Raid，英文全称 Redundant Array of Independent Disks，中文意思“独立磁盘冗余阵列”，有时也简称磁盘阵列（Disk Array）。Raid 是一种把多块独立的磁盘（物理磁盘）按不同的方式组合起来形成一个磁盘组（逻辑磁盘），从而提供比单个磁盘更高的存储性能和数据备份。组成磁盘阵列的不同方式称为 Raid 级别（Raid Levels），常见的 Raid 级别有 Raid0、Raid1、Raid5 和 Raid0+1。

Raid 可以充分发挥出多块磁盘的优势，可以提升磁盘速度，增大容量，提供容错功能，易于管理的优点。在任何一块磁盘（除了 Raid0 意外）出现问题的情况下都可以继续工作，不会受到损坏磁盘的影响。使用 Raid 可以带来以下优点：

- 通过把多个物理磁盘组织在一起作为一个逻辑卷提供磁盘跨越功能。
- 通过把数据分成多个数据块并行写入/读出多个磁盘以提高访问磁盘的速度。
- 通过镜像或校验操作提供容错能力。

1. Raid0

Raid0 是通过将两个或更多磁盘上的可用空间区域合并到一个逻辑卷创建，可以在多个磁盘上分布数据。Raid0 不能被扩展或镜像，不提供容错功能。如果包含 Raid 0 的其中一个磁盘出现故障，则整个逻辑磁盘无法工作。建议使用相同大小、型号和制造商的磁盘。利用 Raid0 可以将数据分块并按一定的顺序写到 Raid0 组成的盘阵中，以分布式存储数据。Raid0 可以同时对所有磁盘进行写数据操作，从而可以相同的速率向所有磁盘写数据，提高数据的写入速度，如图 7-1 所示。

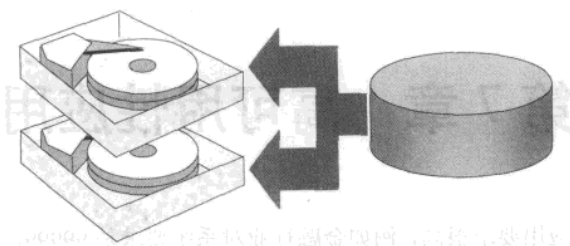


图 7-1 Raid0

(1) 磁盘组。

Raid0 模式，至少需要两块磁盘，可以使用 N 块同样的磁盘用硬件的形式通过智能磁盘控制器或用操作系统中的磁盘驱动程序以软件的方式串联在一起，形成一个独立的逻辑驱动器，容量是单独磁盘的 N 倍，在执行数据写操作时被依次写入到各磁盘中，当一块磁盘的空间用尽时，数据就会被自动写入到下一块磁盘中，它的好处是可以增加磁盘的容量，速度与其中任何一块磁盘的速度相同。

(2) 数据处理。

Raid0 工作状态是把连续的数据分散到多个磁盘上存取。系统数据请求被多个磁盘并行执行，每个磁盘执行属于它自己的那部分数据请求。这种数据上的并行操作可以充分利用总线的带宽，显著提高磁盘整体存取性能。

例如现在有两块磁盘，建立了 Raid0 数据存储模式，数据以 64KB 为单位进行读写，可以同时两块磁盘进行读写，所以 Raid0 对数据的写入、读出速度非常快。一个文件假设有 4 个文件块，第一个块文件写入第一个磁盘，第二个块文件写入第二个磁盘，第三个块文件写入第一个磁盘，第四个块文件写入第二个磁盘，以此类推。数据写入模式如图 7-2 所示。

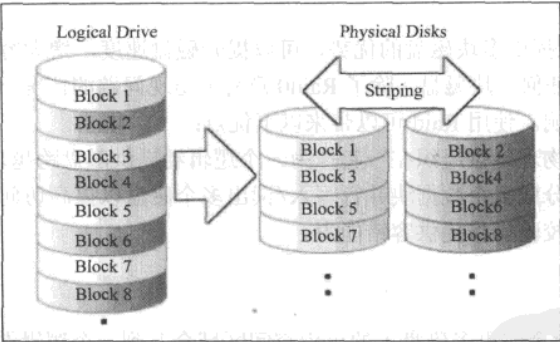


图 7-2 Raid0 数据处理模式

(3) Raid0 的优缺点。

Raid0 连续地分割数据并并行地读/写于多个磁盘上，因此具有很高的数据传输率，但 Raid0 在提高性能的同时，并没有提供数据可靠性，如果一个磁盘失效，因此一旦硬件损坏，损坏的数据将无法恢复。因此 Raid0 不具备数据备份、容错的功能。

尽管不具备容错能力，但 Raid0 在所有数据存储模式中的性能最好，同时它通过在多个磁

盘上分配 I/O 请求从而提高了 I/O 性能。Raid0 在以下情况下提高了性能：

- 从（向）大的数据库中读（写）数据。
- 以极高的传输速率从外部源收集数据。

（4） Raid0 适用环境。

Raid0 数据存储模式，使其特别适用于对性能要求较高，而对数据安全要求较低的领域。对于普通用户，Raid0 也是提高磁盘存储性能的绝佳选择，但 Raid0 不可应用于需要数据高可用性的关键应用。

2. Raid1

Raid1，即磁盘镜像，把一个磁盘的数据镜像到另一个磁盘上，在不影响性能情况下最大限度的保证系统的可靠性和可修复性上，具有很高的数据冗余能力，多用在保存关键性的重要数据的场合。如果一个物理磁盘出现故障，虽然该磁盘上的数据将无法使用，但系统能够继续使用尚未损坏而仍继续正常运转的磁盘进行数据的读写操作，从而通过另一磁盘上保留完全冗余的副本，保护磁盘上的数据免受介质故障的影响，如图 7-3 所示。

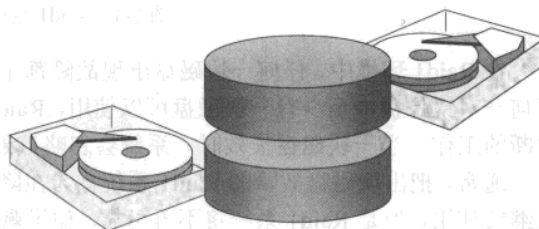


图 7-3 Raid1

（1） 磁盘组。

使用 Raid1，最好使用大小、型号和制造厂家都相同的磁盘，以避免可能产生的兼容性错误。Raid1 可以增强读性能，因为容错驱动程序同时从两个成员中同时读取数据，所以读取数据的速度会有所增加。当然，由于容错驱动程序必须同时向两个成员写数据，所以写性能会略有降低。Raid1 是所有 Raid 等级中实现成本最高的一种。

Raid1，至少需要两块磁盘，两块磁盘建立的镜像容量必须相同。Raid1 的容量等于所选用的磁盘存储空间的总和除以所使用的磁盘数目。在实际工作环境中，Raid1 模式可能用的最多。

（2） 数据处理。

Raid1 是把同一个数据块分别写入到两块不同的磁盘，在执行数据写入时，速度会有一定程度的降低，但是在读出时，是以并发的方式读取，也就是说，读出的速度要远远快于写入的速度。

服务器上现在有两块磁盘，建立了 Raid1。Raid1 的数据是以 64 KB 为单位读写的，一个文件假设有 4 个文件块，第一个块文件写入第一个磁盘，同时第一个块文件写入第二个磁盘，第二个块文件写入第一个磁盘，同时第二个块文件写入第二个磁盘，以此类推。可以看出，Raid1 具备数据备份功能，就是说如果有一块磁盘损坏的情况下，备份的磁盘还可以继续工作保证数据的安全。数据写入模式如图 7-4 所示。

（3） Raid1 的优缺点。

由于对存储的数据进行百分之百的备份，在所有 Raid 级别中，Raid1 提供最高的数据安全保障。同样，因为数据百分之百备份，备份数据占了总存储空间的一半，因而 Raid1 的磁盘空间利用率只有 50%（每组数据有两个成员），所以 Raid1 磁盘使用成本的花费相对较高。

网管天下 网管经验谈

不过，对于服务器系统而言，稳定压倒一切，一旦系统瘫痪，所有数据都将随之而消失，所以，这些代价是非常值得的。

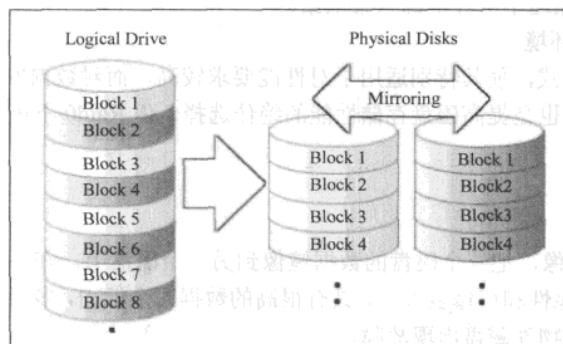


图 7-4 RAID1 数据处理模式

在 RAID1 环境中，任何一块磁盘出现故障都不会影响到系统正常运行，而且只要能够保证任何一对镜像盘中至少有一块磁盘可以使用，RAID1 甚至可以在一半数量的磁盘出现问题时不间断的工作。当一块磁盘失效时，系统会忽略该磁盘，转而使用剩余的镜像盘读写数据。

通常，把出现磁盘故障的 RAID1 系统称为在降级模式下运行。虽然这时保存的数据仍然可以继续使用，但是 RAID1 系统将不再可靠。如果剩余的镜像盘也出现问题，那么整个系统就会崩溃。因此，应当及时的更换损坏的磁盘，避免出现新的问题。更换新盘之后，原有好盘中的数据必须被复制到新盘中，这一操作被称为同步镜像。同步镜像一般需要很长时间，尤其是当损害的磁盘的容量很大时更是如此。在同步镜像进行的过程中，外界对数据的访问不会受到影响，因为复制数据需要占用一部分的带宽，所以可能会使整个系统的性能有所下降。

RAID1 具备以下特点：

- RAID1 的每一个磁盘都具有一个对应的镜像盘，任何时候数据都同步镜像，系统可以从一组镜像盘中的任何一个磁盘读取数据。
- 磁盘所能使用的空间只有磁盘容量总和的一半，成本高。
- 系统中任何一对镜像盘中至少有一块磁盘可以使用，甚至可以在一半数量的磁盘出现问题时系统都可以正常运行。
- 出现磁盘故障的 RAID 系统不再可靠，应当及时的更换损坏的磁盘，否则剩余的镜像盘也会出现问题，整个系统就会崩溃。
- 更换新盘后原有数据会需要很长时间同步镜像，外界对数据的访问不会受到影响，只是这时整个系统的性能有所下降。
- RAID1 磁盘控制器的负载相当大，用多个磁盘控制器可以提高数据的安全性和可用性。

(4) RAID1 适用环境。

RAID1 不能提高存储性能，但由于其具有的高数据安全性，使其尤其适用于存放重要数据，例如服务器和数据库存储等环境中。

3. RAID5

在 RAID5 中，操作系统通过给该卷的每个磁盘分区中添加奇偶校验信息实现容错。如果

某个磁盘出现故障，操作系统便可以用其余磁盘上的数据和奇偶校验信息重建发生故障的磁盘上的数据，如图 7-5 所示。

（1）磁盘组。

Raid5 卷至少需要 3 块磁盘或者更多的磁盘，比前面的几种方式磁盘数量都多。如果使用了 3 块磁盘，那么 Raid5 卷的容量等于所选用的其中两块磁盘的存储空间之和。3 块磁盘建立的 Raid5 方式的容错所需的存储空间必须相同。Raid5 卷的数据是以 64 KB 为单位读写的。

（2）数据处理。

Raid5 卷是把数据块按顺序的写入不同的磁盘中，在执行数据写入、读取时以并发的方式操作，也就是说，写入、读取速度非常快，同时 Raid5 卷具备容错功能。

由于要计算奇偶校验信息，Raid5 写操作要比 Raid1 写操作慢一些。但是，Raid5 比 Raid1 提供更好的读性能，操作系统可以从多个盘上同时读取数据。与 Raid1 相比，Raid5 的性价比较高，而且 Raid5 卷中的磁盘数量越多，冗余数据带区的成本越低，因此，Raid5 被广泛应用于数据存储。Raid5 数据存储也有一些限制，例如 Raid5 卷至少需要 3 个磁盘才能实现，但最多不能超过 32 个磁盘。

一个文件假设有 6 个文件块，第一个块文件写入第一个磁盘，第二个块文件写入第二个磁盘，第一个、第二个块文件写入成功以后，Raid5 根据系统提供的奇偶校验算法对第一个文件块和第二个文件块进行计算，得出一个奇偶校验值，把这个值写入第三块磁盘中。也就是说现在的磁盘 3 上存储的不是第三个块文件，而是校验信息；然后第三个块文件写入第一个磁盘，第四个块文件写入第二个磁盘，第二个磁盘上存储的是第三个、第四个块文件的奇偶检验信息；然后第五个块文件写入第二个磁盘，第六个块文件写入第三个磁盘，第一个磁盘上存储的是第五个、第六个块文件的奇偶检验信息，以此类推。从以上的存储算法看出，Raid5 卷具备数据容错功能，就是说如果有一块磁盘损坏的情况下，更换磁盘以后，可以根据奇偶校验算法反算出损坏的那块磁盘的数据，保证数据的安全。如果这个例子中的两块磁盘出现了问题，数据也会全部丢失。数据写入如图 7-6 所示。

（3）Raid5 优缺点。

Raid5 可以理解为是 Raid 0 和 Raid 1 的折衷方案。Raid 5 可以为系统提供数据安全保障，但保障程度要比 Raid1 低而磁盘空间利用率要比 Raid1 高。Raid 5 具有和 Raid 0 相近似的数据读取速度，只是多了一个奇偶校验信息，写入数据的速度比对单个磁盘进行写入操作稍慢。同时由于多个数据对应一个奇偶校验信息，Raid5 的磁盘空间利用率要比 Raid1 高，存储成本相对较低。

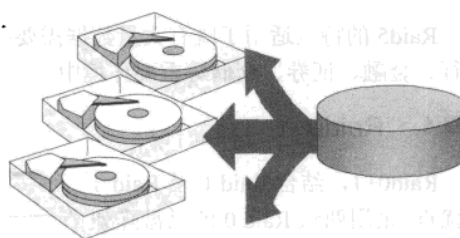


图 7-5 RAID5

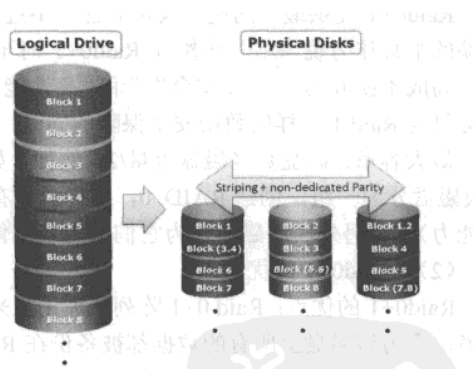


图 7-6 Raid5 数据处理模式

网管天下 网管经验谈

（4） Raid5 适用环境。

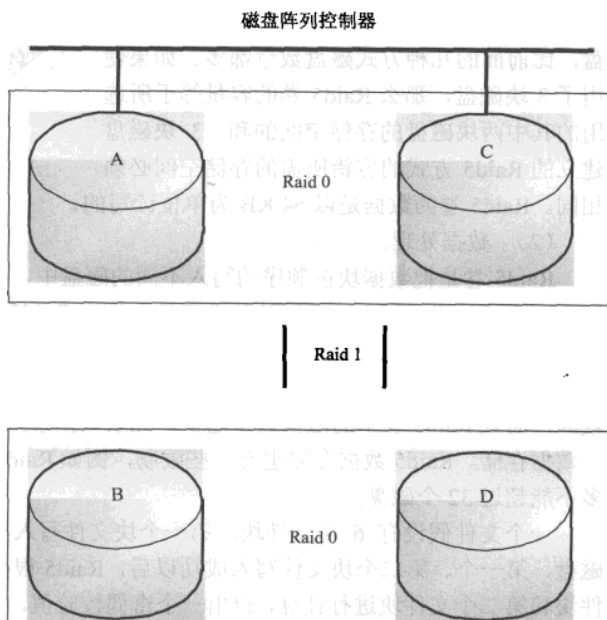
Raid5 的特点适用于既有大量数据需要存取，同时又对数据安全性要求严格的领域，例如银行、金融、证券、仓储等重要环境中。

4. Raid0+1

Raid0+1，结合 Raid 0 及 Raid 1 的优点，采用两组 Raid 0 的磁盘阵列互为镜像，也就是它们之间又成为了一个 Raid 1 的阵列。在每次写入数据时，磁盘阵列控制器会将数据同时写入两组“大容量阵列磁盘组”（Raid0）中。数据除分布在多个盘上外，每个盘都有其物理镜像盘，提供全冗余能力，允许一个以下磁盘故障，而不影响数据可用性，并具有快速读/写能力。

（1） 磁盘组。

至少 4 个磁盘才能做成 Raid0+1。如果是 4 块磁盘 A、B、C、D 部署 RAID0+1 方案，可以使用磁盘 A、C 部署为 Raid0，磁盘 B、D 建立部署为 Raid0，然后将两个 Raid0 部署为 Raid1，如图 7-7 所示。



Raid0+1 提供最佳的速度及可靠性。不过需要两倍的磁盘驱动器数目作为一个 Raid0，每一端的半数作为镜像用。在执行 Raid0+1 时至少需要 4 个磁盘驱动器，所以可以说 Raid0+1 通过高成本换取的是“高安全性”和“高性能”。Raid 0+1 是存储性能和数据安全兼顾的方案，在提供与 Raid 1 一样的数据安全保障的同时，也提供了与 Raid 0 近似的存储性能。

最大容量：磁盘数×磁盘容量/2。例如，如果有 6 块磁盘希望使用 Raid0+1 模式，可以将 3 块磁盘分为一组，创建 RAID 0，这样总体存储性能就是每块磁盘的 3 倍（磁盘数×磁盘存储能力）。将另外 3 块磁盘作为它们的内容镜像。

（2） Raid0+1 的优缺点。

Raid0+1 的优点：Raid 0+1 阵列从理论上来说，能够经受住 Raid 0 阵列中任何一块磁盘的故障，因为该磁盘上所有的数据都被备份在 Raid 1 阵列中。在大部分情况下，如果两块磁盘出现故障就会影响整个阵列，因为很多 Raid 控制器会在 Raid 阵列中的某一块磁盘出现故障之后让 Raid 0 镜像离线（Raid 0 阵列不提供任何冗余），因此只有剩下的 Raid 0 阵列在工作，这样系统将不存在冗余功能。简而言之，如果每个 Raid 0 阵列中都有一块磁盘出现故障，那么整个磁盘阵列将不工作。Raid0+1 提供了非常好的顺序或任意读写的性能。

Raid0+1 的缺点：只能使用磁盘阵列总体存储容量的 50%。容错性不如 Raid 1+0。对于绝大部分控制器来说，这种模式能够应对一块磁盘出现故障的情况。扩展方面受到限制，而且扩展的费用很高。

(3) Raid0+1 适用环境。

Raid 0+1 的特点使其特别适用于既有大量数据需要存取,同时又对数据安全性要求严格的领域,例如银行、金融、档案管理等环境中。

5. Raid1+0

Raid1+0, 由两组 Raid1 的磁盘做 Raid0 的镜像完成容错功能。Raid1+0 的磁盘空间利用率和 Raid0+1 相同。其他参数数字可以参考 Raid0+1 部分内容, Raid1+0 部署结构 (4 块磁盘为例说明), 如图 7-8 所示。

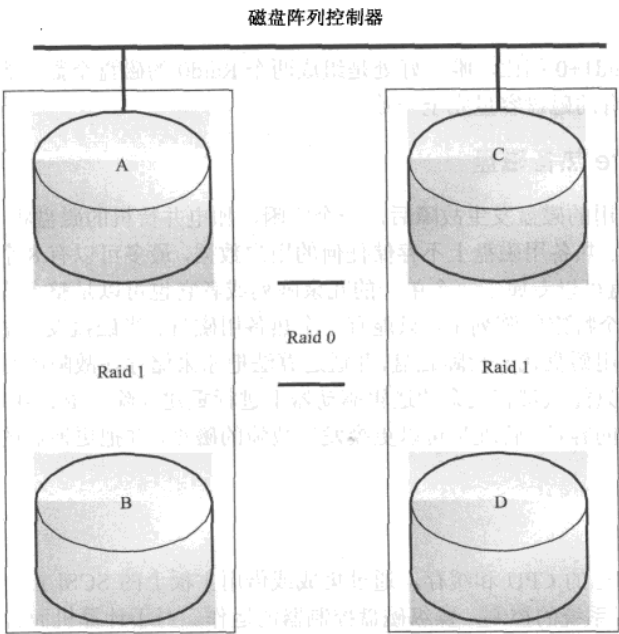


图 7-8 Raid1+0 架构

6. Raid0+1 与 Raid1+0 的区别

Raid0+1 与 Raid1+0 虽然都利用了 Raid0 和 Raid1 的优点,但两种架构之间存在区别,因此在数据安全性上也存在区别。

(1) Raid 结构。

从结构上来看,如果两种 Raid 都是由 4 块物理磁盘组成,分别定义为 A 盘、B 盘、C 盘、D 盘。那么 Raid0+1 是先有两组 Raid0, 第一组 Raid0 (命名为 AB) 由 A 和 B 组成, 第二组 Raid0 (命名为 CD) 由 C 和 D 组成, 然后再由 AB 和 CD 组成 Raid1, 即两组 Raid0 间是互为镜像的关系; 而 Raid1+0 是先有两组 Raid1, 第一组 Raid1 (命名为 AB) 由 A 和 B 组成, 第二组 Raid0 (命名为 CD) 由 C 和 D 组成, 然后再由 AB 和 CD 组成 RAID0, 两组 RAID1 之间是不带校验的条带关系。

网管天下 网管经验谈

（2）数据安全性。

若有磁盘出现物理问题时，两种 Raid 的可靠性可存在着相当大的差别。在 Raid0+1 中，若有一块磁盘（假设为 A 盘）出现物理问题时，A 盘所在的 AB 组 Raid0 也就不再工作，只剩下 CD 一组 Raid0 提供服务，此时的安全性可想而知；而在 Raid1+0 中，若同样有一块磁盘（假设为 A 盘）出现物理问题，除 A 盘以外，其他磁盘一样正常提供服务，虽然可靠性有所降低，但仍要强于第一种情况下的 Raid0。当然当组成 Raid 的磁盘个数增加时，这种可靠性的差距会更大。

（3）性能。

相比而言 Raid1+0 比 Raid0+1 具有更高的可用性，而性能上几乎没有差异。

（4）磁盘组成。

Raid0+1 与 Raid1+0 相比，唯一好处是组成两个 Raid0 的磁盘个数和容量可以不一致，而 Raid1+0 则要求所有的磁盘容量完全一致。

7. HotSpare 热备磁盘

当一个正在使用的磁盘发生故障后，一个空闲、加电并待机的磁盘将马上代替此故障盘，此方法就是热备用。热备用磁盘上不存储任何的用户数据，最多可以有 8 个磁盘作为热备用磁盘。一个热备用磁盘可以专属于一个单一的冗余阵列或者它也可以是整个阵列热备用磁盘池中的一部分。而在某个特定的阵列中，只能有一个热备用磁盘。当磁盘发生故障时，控制器的固件能自动的用热备用磁盘代替故障磁盘，并通过算法把原来储存在故障磁盘上的数据重建到热备用磁盘上。数据只能从带有冗余的逻辑驱动器上进行重建（除了 Raid0 以外），并且热备用磁盘必须有足够多的容量。管理员可以更换发生故障的磁盘，并把更换后的磁盘指定为新的热备用磁盘。

8. Raid 卡

Raid 卡拥有自己的 CPU 和缓存，通过集成或借用主板上的 SCSI 控制器管理磁盘，独立实现对 Raid 存储子系统的控制，操纵磁盘控制器的运作。对于计算机而言，Raid 卡上无论连接多少块磁盘，都将显示为一块逻辑磁盘，而 Raid 控制器则表现如同一个 SCSI 控制器。由于 Raid 控制器独自处理所有的实际磁盘通信，在向 Raid 控制器中插入磁盘时，就像插入到 SCSI 控制器一样，操作系统并不知道配置有所变化。

如果服务器内置有 Raid 芯片，无需再另行安装 Raid 卡。硬件 Raid 可以极大地节约服务器系统 CPU 和操作系统的资源，从而使网络服务器的性能获得很大提高。在检测和修复多位错误的能力、Raid 保护的可引导阵列、错误磁盘自动检测、剩余空间取代和阵列重建、共有的或指定的剩余空间和彩色编码报警等许多方面，都是软件 Raid 所无法比拟的。

SCSI Raid 卡应当安装 SCSI 接口磁盘，而 SATA Raid 卡则应当连接 SATA 磁盘。另外，Raid 卡所支持的标准必须与磁盘的标准一致，并且磁盘必须选择同一厂商和同一型号的产品。

7.1.2 BIOS 设置 Raid 卡

目前服务器系统中，基本都内置了 Raid 卡，服务器的型号不同内置的 Raid 卡也不同。部分产品提供服务器快速安装向导，管理员根据向导即可完成 Raid 的设置。对于没有提供安装

高可用性应用 | 7

向导的服务器，通过 BIOS 也可以设置 Raid。下面以 Dell PowerEdge 2650 为例说明如何设置和安装 Raid 卡。不同 Raid 卡的设置方式有所区别，请注意查看 Raid 卡的使用手册。

第 1 步，打开计算机电源，当显示如图 7-9 所示提示信息时，按下“Ctrl+M”组合键，进入 Raid 卡设置页面。

第 2 步，使用光标键，选择“Configure → Easy Configuration”选项，并按 Enter 键，实现 Raid 卡的快速配置，如图 7-10 所示。

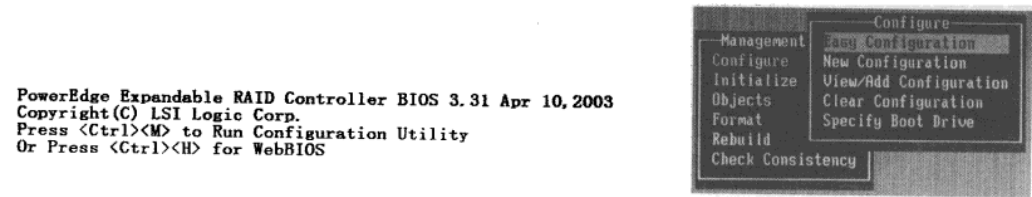


图 7-9 提示 RAID 卡设置组合键

图 7-10 采用 Easy Configuration 方式

提示 如果该计算机以前配置有 Raid，那么，在配置新的 Raid 之前，应当先使用“Clear Configuration”命令删除。Raid 删除后，磁盘中保存的所有数据将全部丢失。

第 3 步，Raid 卡自动搜索并显示该计算机中安装的所有磁盘驱动器，如图 7-11 所示。
第 4 步，使用光标键选择欲添加至 Raid 的磁盘，按下空格键选中，将该磁盘添加至 Raid 阵列，如图 7-12 所示。

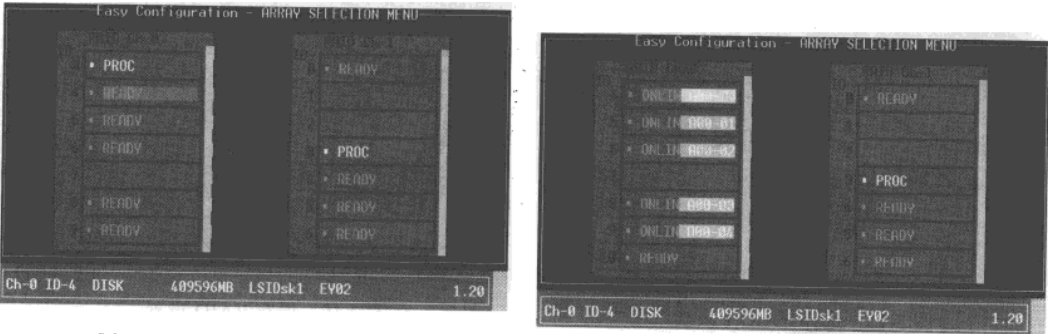


图 7-11 显示所有的磁盘驱动器

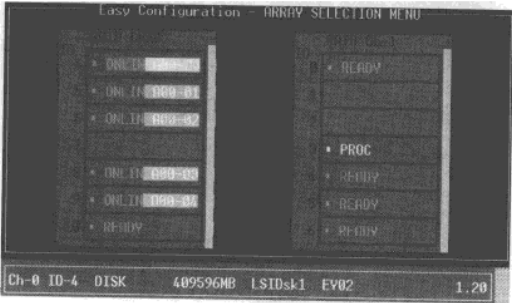


图 7-12 选择欲添加至 Raid 的磁盘

提示 若欲设置 Raid5，为了最大限度地利用磁盘空间利用率，应当将所有的磁盘都加入至 Raid。若欲设置 Raid1，则需要添加两块磁盘。

第 5 步，按下 Enter 键，显示如图 7-13 所示页面，使用光标键选择欲配置的阵列。如果只使用了一个通道，选择“Span-1”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 6 步，按下“F10”键，显示如图 7-14 所示页面，选择欲使用的 Raid 级别。当计算机安装有 3 块以上磁盘时，系统默认的级别为 Raid5。

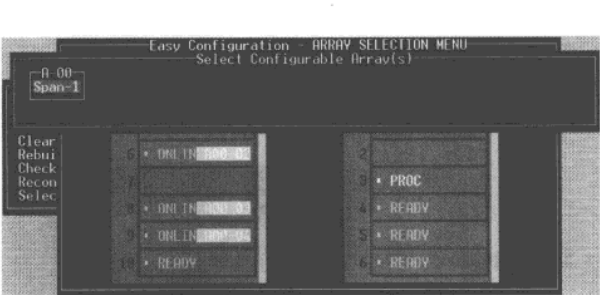


图 7-13 选择 RAID 卡通道

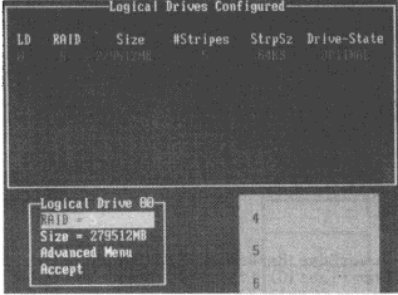


图 7-14 选择 RAID 5 级别

当服务器只安装有两块磁盘时，则默认级别为 Raid1，如图 7-15 所示。

提示 若欲设置为其他级别，可以使用光标键使“Raid=”反亮显示，然后进行修改。

第 7 步，移动光标使“Accept”反亮显示，并按 Enter 键，系统提示是否保存设置如图 7-16 所示。移动光标使“YES”反亮显示并按 Enter 键，即可完成 Raid 卡的设置。

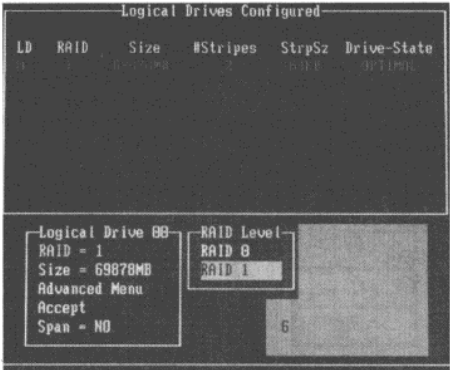


图 7-15 选择 RAID 1 级别

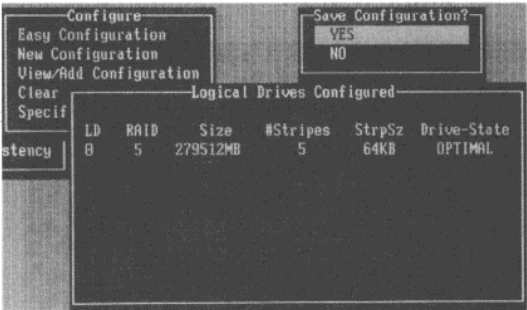


图 7-16 保存 RAID 设置

第 8 步，根据系统提示，重新引导计算机，即可完成 Raid 的设置。

7.2 网卡高可用性

网卡是计算机和外部（网络或者 Internet）联系的主要通道。个人计算机默认安装一块网卡，服务器基本配置为安装两块网卡，网卡的速率根据服务器的型号将有所不同，可能为：100 MB、1 GB 或者 10 GB。

7.2.1 网卡数量

如果在服务器中仅安装一块网卡，建议管理员至少增加一块网卡。一块为主网卡，其他的作为备用网卡，然后通过多根网线将多块网卡连到同一交换机。在服务器和交换机之间建立主连接和备用连接。通过虚拟网卡软件（NICExpress）将多块网卡绑定为一块网卡，或者称之为虚拟网卡组，然后为虚拟网卡组设置一个唯一的 IP 地址。

计算机安装多网卡后，通过多网卡并发方式传输数据，将提高网络传输效率，提高系统性能。一旦虚拟网卡组的任何一个物理链接断开（网卡出现故障或者链路断开），系统软件将自动监测链接状态，出现故障的网卡将自动切换到其他网卡物理链接，通常用户不会觉察到任何变化。

7.2.2 多网卡优点

计算机中部署多块网卡后，将带来以下优点：

- 带宽增容。如果计算机中使用 3 块 100 MB 网卡，理论上 3 块网卡的传输带宽就是 300 MB。实际效果不能根据网卡数量，经过简单叠加后就认为是计算机网络带宽。经过实测，3 块网卡传输总带宽可以达到 250 MB 左右。
- 负载均衡。多块网卡被虚拟成“一块网卡”之后，虚拟网卡软件协调网卡之间同步工作，经过服务器的数据流（流入、流出）被分配到不同网卡，减轻每块网卡的网络负载，增强服务器并发访问能力，提高服务器性能。
- 故障自动转移。如果服务器中的任何一块网卡出现故障，其他网卡将自动接管出现故障的网卡，该处理过程在后台自动完成，服务器中的系统服务或者应用不会中断，增强服务器的可用性。
- 网卡冗余阵列。将服务器上安装的所有网卡虚拟成一个阵列组，或者称之为虚拟网卡组，每个物理链接由系统软件自动分配数据流量。

7.2.3 部署虚拟网卡

在计算机中安装多网卡时，建议选择遵循以下标准：

- 支持最大网卡数量，管理员可以参考计算机配置和管理软件支持的最大数量。
- 网卡型号相同。
- 所有网卡建议连接到同一台交换机。

以 NICExpress 虚拟网卡软件实际部署为例，说明如何部署虚拟网卡。NICExpress 软件安装过程就是配置过程，软件安装完成后，即可正常使用。

第 1 步，从网上下载 NICExpress 虚拟网卡软件，双击启动程序安装，显示如图 7-17 所示的对话框。

第 2 步，检测通过后，显示如图 7-18 所示的“Welcome to NICExpress Enterprise Edition Setup”对话框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

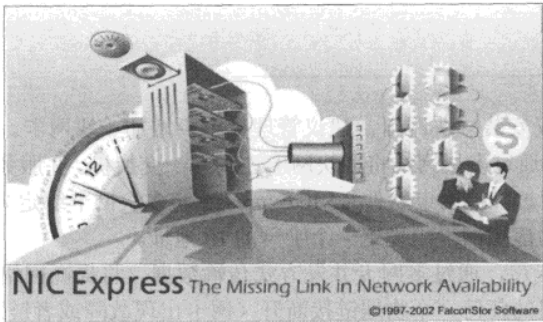


图 7-17 安装 NICExpress 软件之一

第 3 步，单击“Next”按钮，显示如图 7-19 所示的“License Agreement”对话框。

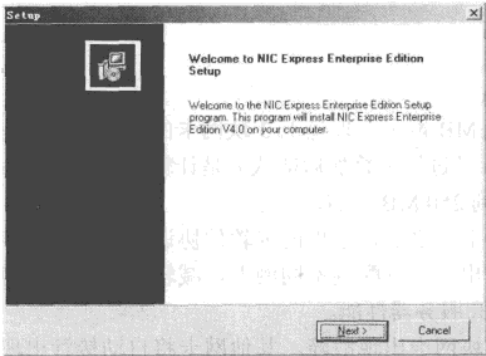


图 7-18 安装 NICExpress 软件之二

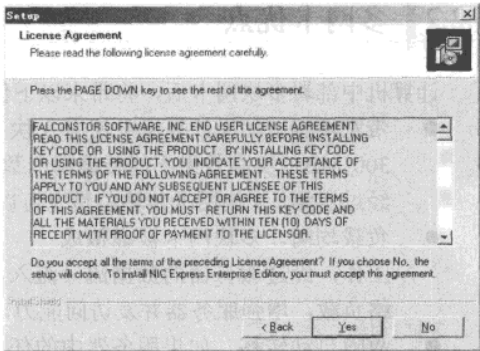


图 7-19 安装 NICExpress 软件之三

第 4 步，单击“Yes”按钮，显示如图 7-20 所示的“Setup Type”对话框。提示是否开启“Load Balancing”功能，即负载均衡功能。选择“Enabled”单选按钮，启用负载均衡功能。

第 5 步，单击“Next”按钮，显示如图 7-21 所示的“Choose Destination Location”对话框，选择安装的目标文件夹。

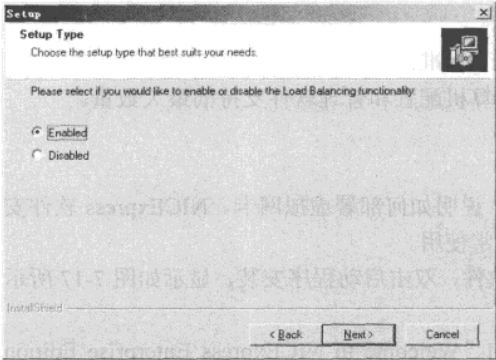


图 7-20 安装 NICExpress 软件之四

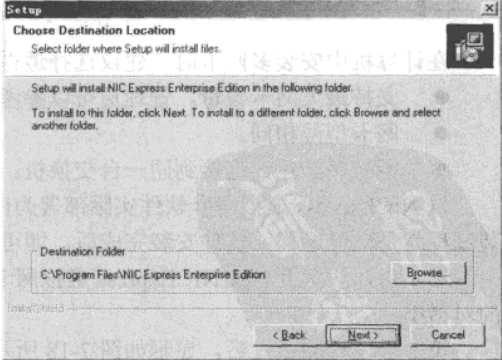


图 7-21 安装 NICExpress 软件之五

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 步，单击“Next”按钮，显示如图 7-22 所示的“Select Program Folder”对话框。设置 NICExpress 虚拟网卡软件在程序文件夹中的名称。

第 7 步，单击“Next”按钮，开始文件复制进程，显示如图 7-23 所示的“Setup Status”对话框。

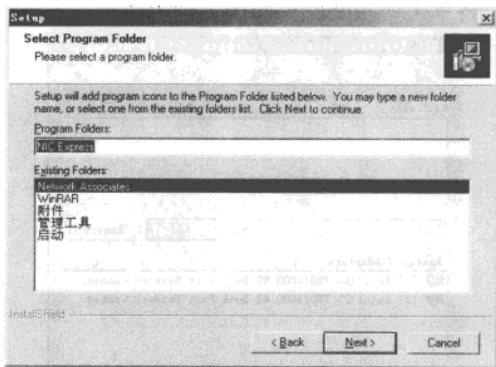


图 7-22 安装 NICExpress 软件之六

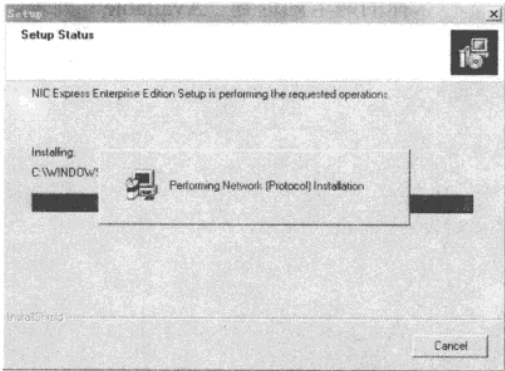


图 7-23 安装 NICExpress 软件之七

第 8 步，文件复制完成后，显示如图 7-24 所示的“Thank you for trying NICExpress”对话框。

第 9 步，本例中单击“Demo”按钮，显示如图 7-25 所示虚拟网卡属性设置对话框。此对话框分为 3 个编辑区域：

- ① “Available” 列表框，已经安装在服务器中所有网卡设备。
- ② 虚拟网卡名称设置区域：在多网卡绑定完成后，显示在网络链接窗口中网卡名称。本例名称虚拟网卡名称为 Test。
- ③ “Assigned Adapters” 列表框，选择需要绑定的网卡列表。

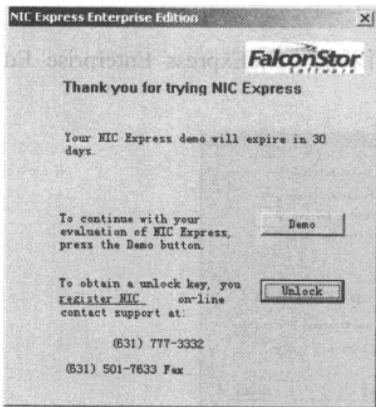


图 7-24 安装 NICExpress 软件之八

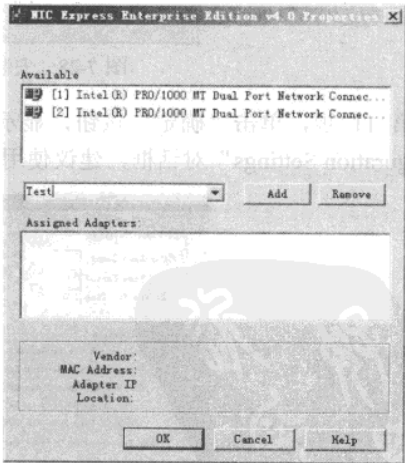


图 7-25 安装 NICExpress 软件之九

- 选择“Available”列表中需要加入到虚拟网卡组“Test”中的网卡设备，单击“Add”

网管天下 网管经验谈

按钮，如果选择的网卡设备已经设置 IP 地址，显示如图 7-26 所示的“Add Adapter”对话框，提示是否使用当前网卡的 IP 地址作为虚拟网卡的 IP 地址。

- 被选择的网卡设备就被自动加入到“Assigned Adapters”列表。如果选择的网卡出现错误，在“Assigned Adapters”列表选择目标网卡，单击“Remove”按钮，被选择的网卡回退到“Available”列表。网卡设备添加完成后，如图 7-27 所示。

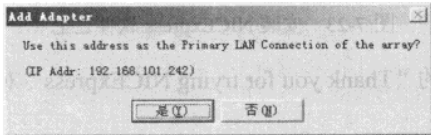


图 7-26 安装 NICExpress 软件之十

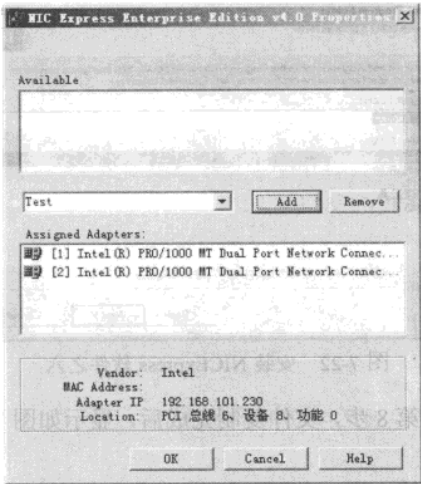


图 7-27 安装 NICExpress 软件之十一

第 10 步，单击“OK”按钮，显示如图 7-28 所示的“Information”信息提示对话框。提示网络管理员需要进行网卡属性设置。

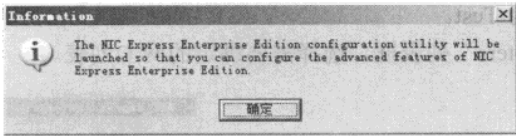


图 7-28 安装 NICExpress 软件之十二

第 11 步，单击“确定”按钮，显示如图 7-29 所示的“NicExpress Enterprise Edition Configuration Settings”对话框，建议使用默认值即可。

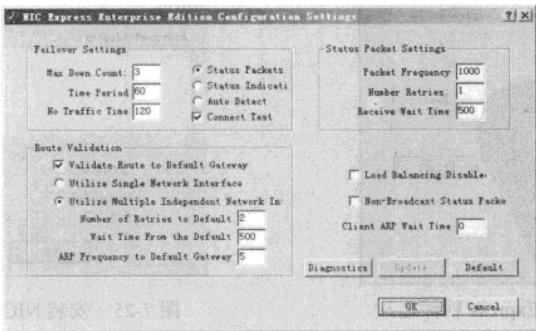


图 7-29 安装 NICExpress 软件之十三

第 12 步，单击“OK”按钮，显示如图 7-30 所示的“Setup Complete”对话框。

第 13 步，单击“Finish”按钮，完成软件的安装。NICExpress 虚拟网卡软件安装完成后，打开“网络连接”窗口，如图 7-31 所示。原服务器中网卡连接为两个，配置完成后增加了一个网卡连接图标，共计为三个，多出来的一个图标名称是“NIC Express Virtual Adapter”，适配器的名称为 Test，即新建立的虚拟网卡组。虚拟网卡组的使用和使用单一网卡完全一样，相当于一个单一的网卡。

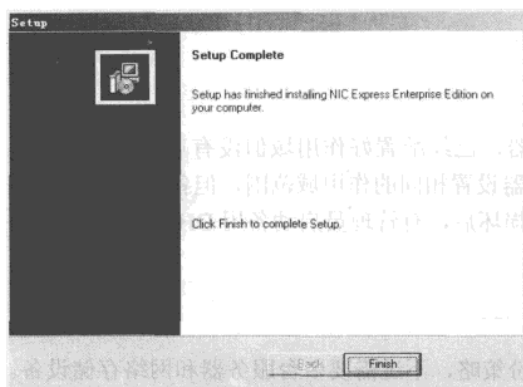


图 7-30 安装 NICExpress 软件之十四

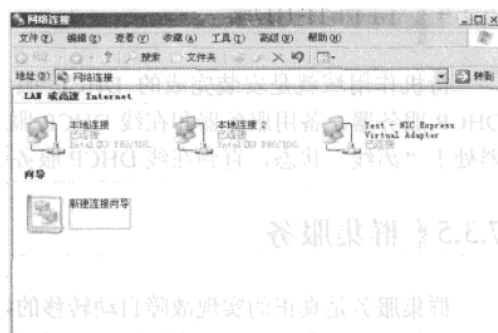


图 7-31 安装 NICExpress 软件之十五

7.3 DHCP 高可用性应用建议

在实际应用中，至少要部署两台 DHCP 服务器。如果整个网络中只有 1 台 DHCP 服务器，当 DHCP 停止工作时，网络中的工作站可能获取不到 IP 地址，从而引起网络中断。为了提高容错能力，在条件允许的情况下，推荐在网络中部署两台 DHCP 服务器。

7.3.1 DHCP 容错 50/50 故障转移

DHCP 容错的 50/50 故障转移方法，需要两台 DHCP 服务器，每台服务器处理同等数量的客户端请求。每台服务器采用同样的作用域配置，但作用域的范围不能重叠，以避免 IP 地址冲突。每台服务器覆盖整个网络中所有 IP 地址的范围，第一台服务器的作用域被配置成排除了指定端的所有 IP；第二台服务器的作用域被设置成其他 IP 地址的范围。

7.3.2 DHCP 容错 80/20 故障转移

80/20 规则是最常见的 DHCP 地址分配方法。该规划也使用两个 DHCP 服务器。各网段的 DHCP 遵循 80/20 原则，即本地网段的 80% 地址由本地网段的 DHCP 负责，其余 20% 的地址由另一个网段的 DHCP 负责。具体实现的方法是将负责本地网段的 DHCP 上排除掉那 20% 的地址，另一个网段的 DHCP 上排除掉那 80% 的地址。

7.3.3 DHCP 容错 100/100 故障转移

DHCP 容错 100/100 故障转移包括两台 DHCP 的服务器，每台服务器都为公司的同一个子网分配 IP 地址，但是，每台服务器上的作用域包含有地址不同而容量相同的 IP 范围，如果两台服务器中的一台服务器中断后，第二台服务器将会接管工作，对客户端做出响应，但是客户端得到的是不同的 IP 地址。

7.3.4 待机作用域

待机作用域就是安装完成的 DHCP 服务器，已经配置好作用域但没有启用，作为备用 DHCP 服务器。备用服务器和在线 DHCP 服务器设置相同的作用域范围，但备用 DHCP 服务器处于“离线”状态，直到在线 DHCP 服务器损坏后，有管理员启动备用 DHCP 服务器。

7.3.5 群集服务

群集服务是真正的实现故障自动转移的备份策略，不过需要多台服务器和网络存储设备。当其中的任何一台 DHCP 服务器出现故障后，将自动转移到其他的 DHCP 服务器中，不需要管理员干预，切换过程对管理员和客户端用户来说完全透明。缺点是需要高昂的硬件设备。

7.4 域控制器高可用性

域控制器是运行 Windows Server 网络中最重要的组件，域控制器是否稳定直接决定网络工作是否正常。域控制器和其他服务器的区别在于域控制器运行 AD DS 域服务，提供最基础的用户管理、计算机管理、组策略管理、权限管理等基础运营平台。如果域控制器出现故障，用户将不能访问网络资源。

7.4.1 域控制器概述

域控制器是运行 AD DS 域服务的服务器，AD DS 域服务是 Windows Server 2008 提供目录服务，要部署 AD DS 域服务首先需要安装 Active Directory Domain Services 服务器角色。AD DS 域服务角色安装完成后直接使用“Active Directory 域服务安装向导”或者使用“Dcpromo”命令行将当前的服务器提升为域控制器。AD DS 域服务是真正的服务，和 WWW 服务相同，域管理员可以停止、启动该服务，这也是 AD DS 域服务和 Windows Server 2000/2003 的 Active Directory 最大不同的地方。要了解域控制器，首先需要了解几个关于服务器的概念。

1. 独立服务器

安装完成 Windows Server 2008 操作系统后，运行该操作系统的计算机就成为一台独立服务器。该服务器可以独立部署应用程序，最明显的特征是该服务器没有加入到“域”中。如果要部署网络中的第一台域控制器，可以在独立服务器的基础上使用“Dcpromo.exe”命令，直

接提升为域控制器。

■ 2. 成员服务器

独立服务器添加到“域”中之后，就成为成员服务器。该服务器接受 AD DS 域服务的统一管理，接收并应用 Active Directory 发布的组策略，该计算机被添加到“Computers”组织单位中。如果要在网络中部署额外域控制器或者子域，首先需要将独立服务器提升为成员服务器，在成员服务器的基础上运行“Dcpromo.exe”命令，将成员服务器提升为额外域控制器或者子域。

■ 3. 域控制器

网络中第一台部署 AD DS 域服务的服务器，就是域控制器。域控制器和额外域控制器之间存在区别，虽然二者都是域控制器，但是在域控制器中运行操作主机角色的分别为：架构主机角色、域命名主机计算机、PDC 主机角色、RID 主机角色和结构主机角色，同时域控制器也是默认的全局编录服务器。

■ 4. 额外域控制器

成员服务器使用“Dcpromo”命令行工具或者添加“AD DS 域服务”角色后，将被提升为额外域控制器，该计算机被添加到“Domain Controllers”组织单位中。在服务器上运行“AD DS 域服务”，提供管理任务，存储 Active Directory 数据库。额外域控制器是域控制器的备份服务器。

■ 5. AD DS 域服务

AD DS 域服务全称 Active Directory Domain Services，和 Windows Server 2000/2003 的 Active Directory 有本质的区别，以前版本的 Active Directory 以应用程序的方式体现，在域控制器正常运行时不能对 Active Directory 数据库进行维护。Windows Server 2008 AD DS 域服务是一种真正意义上的服务，域管理员可以随时“停止”或者“启动”AD DS 服务，具备普通服务的所有特性。域管理员可以在命令行模式或图形模式完成服务的管理。

AD DS 域服务是 Windows Server 2008 网络中最基础也是最重要的网络基础平台，将管理网络中的 IT 资源，包括用户、计算机、联系人、域控制器、组策略、信任关系、复制、组织单位、组、共享文件夹、打印机等系列网络资源，这些信息存储在 Active Directory 数据库中。维护和保证 Active Directory 数据库的正常运行，是管理员最重要的工作。以 AD DS 域服务为基础，将拓展系列应用，例如 Exchange Server、Microsoft SQL Server 数据库、IIS 等。

AD DS 域服务不仅可以在安装完整版本的 Windows Server 2008 下运行，也可以在 Windows Server 2008 Server Core 中运行，在 Server Core 部署 AD DS 域服务需要使用脚本文件部署。Server Core 是 Windows Server 2008 系统中的一个独立的核心功能，该组件不同于完整模式的 Windows Server 2008 系统，没有图形界面，管理功能全部在“DOS 命令提示符”模式中完成，提供特定 Windows 核心基础服务。安全性、稳定性是部署 Server Core 系统追求的目标。

■ 6. 域控制器故障转移

网络中部署 Windows Server 2008 AD DS 域服务的域控制器时，建议至少部署一台额外域控制器，这样即使域控制器出现故障，管理员可以在短时间之内将域控制器中的操作主机角色

网管天下 网管经验谈

和全局编录服务迁移到额外域控制器中，确保 AD DS 域服务的正常运行。一旦 AD DS 域服务出现故障，客户端计算机将不能登录到域中，将无法访问域内的资源，以及无法使用组策略等高级管理功能，电子邮件服务器（Exchange Server）将无法确认目标接收者，即无法正常收发电子邮件。

7.4.2 部署域控制器

部署 Windows Server 2008 域控制器前，需要首先安装 Windows Server 2008 操作系统，然后完成以下任务：重命名服务器，更改服务器的 IP 地址，设置网络类型，然后安装 AD DS 域服务。安装 AD DS 域服务分两个阶段：安装角色和提升域服务。

1. 网络参数设置

Windows Server 2008 安装完成后，网络参数需要管理员手动设置。默认安装的 Windows Server 2008 同时启用 IPv4 和 IPv6 两种协议，在安装 AD DS 域服务时，不建议同时启用两种协议，选择一种即可。如果安装过程中需要同时安装 Active Directory 集成区域 DNS 服务器，将“首选 DNS 服务器”IP 地址指向当前服务器 IP 地址。

2. 部署 AD DS 域服务

Windows Server 2008 操作系统安装完成后，并没有自动安装 AD DS 域服务，需要管理员首先安装“AD DS 域服务”角色，然后使用“Dcpromo.exe”工具将独立服务器提升为域控制器。

第 1 步，选择“开始”→“管理工具”→“服务器管理器”选项，显示如图 7-32 所示的“服务器管理器”窗口。

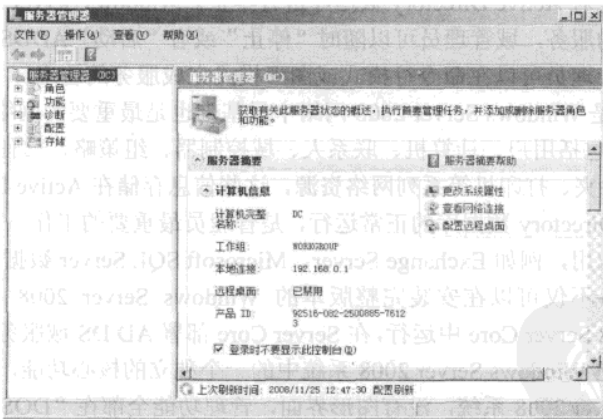


图 7-32 部署 AD DS 域服务之一

第 2 步，选择“服务器管理器”→“角色”选项，显示如图 7-33 所示的“服务器管理器”窗口。

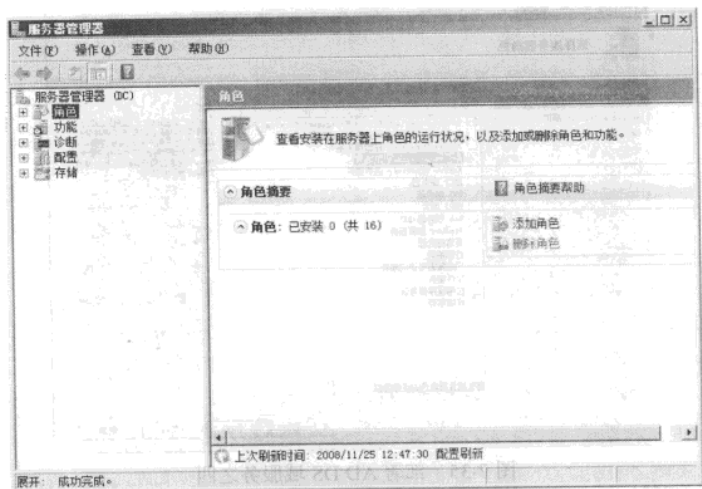


图 7-33 部署 AD DS 域服务之二

第 3 步，在右侧窗口中，单击“添加角色”超链接，显示如图 7-34 所示的“开始之前”对话框，提示管理员安装角色注意事项。

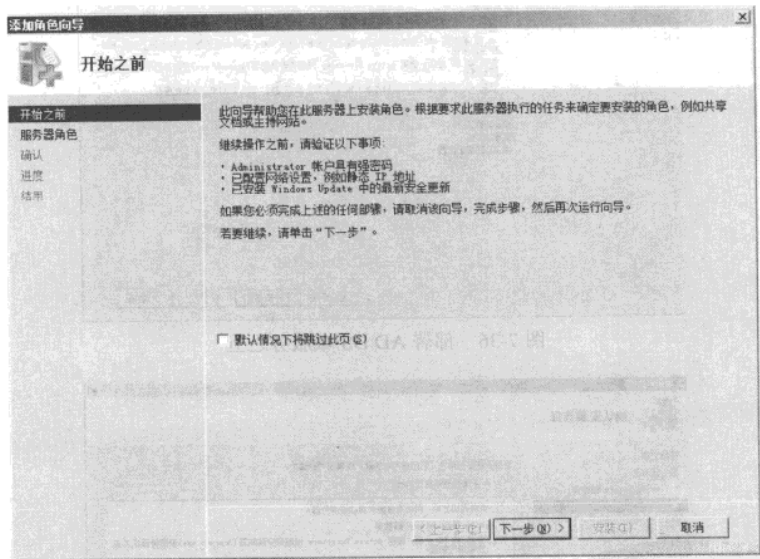


图 7-34 部署 AD DS 域服务之三

第 4 步，单击“下一步”按钮，显示如图 7-35 所示的“选择服务器角色”对话框。在“角色”列表框中，选择“Active Directory 域服务”复选框。

第 5 步，单击“下一步”按钮，显示如图 7-36 所示的“Active Directory 域服务”对话框，简要介绍 Active Directory 域服务的作用和功能。

第 6 步，单击“下一步”按钮，显示如图 7-37 所示的“确认安装选择”对话框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

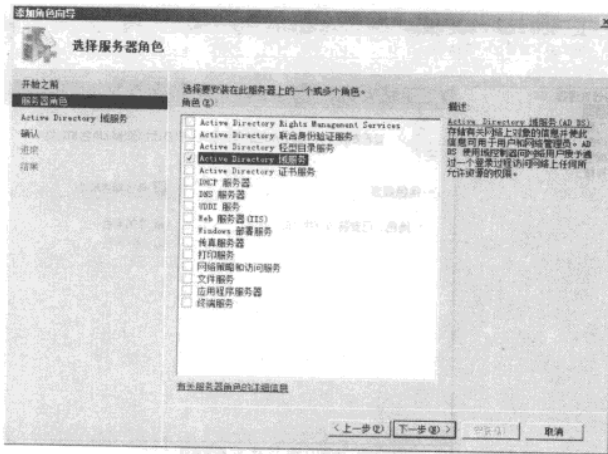


图 7-35 部署 AD DS 域服务之四

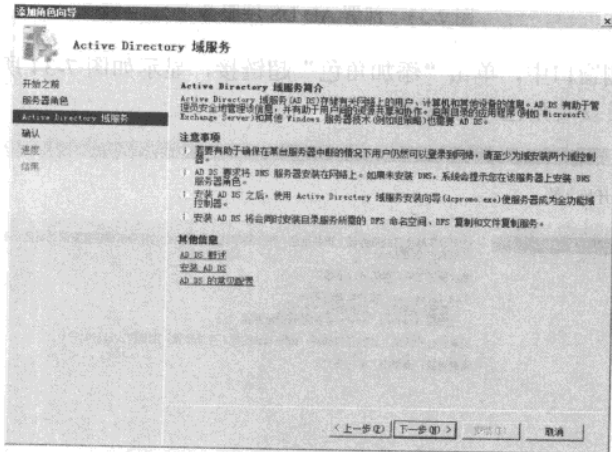


图 7-36 部署 AD DS 域服务之五

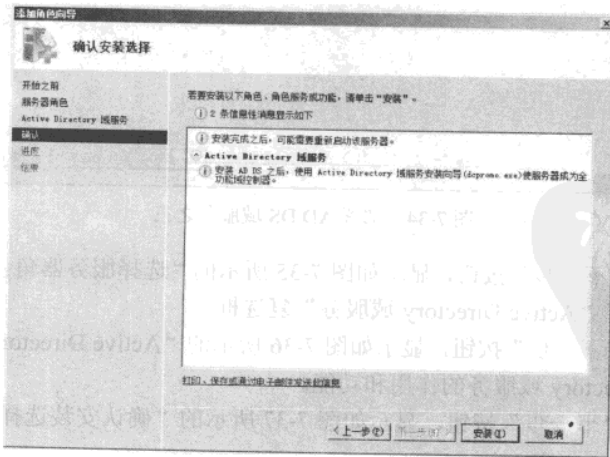


图 7-37 部署 AD DS 域服务之六

第 7 步，单击“安装”按钮，显示如图 7-38 所示的“安装进度”对话框，并显示安装进度。

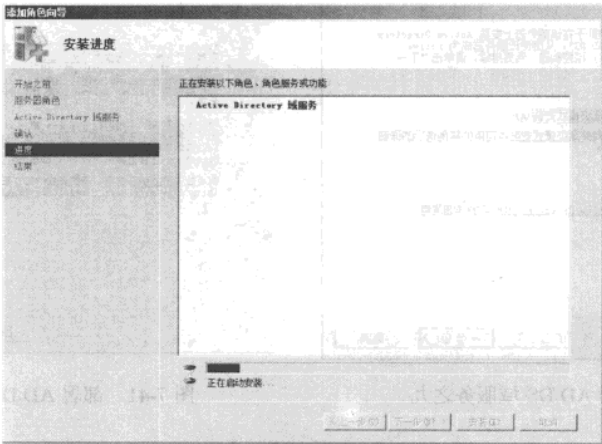


图 7-38 部署 AD DS 域服务之七

第 8 步，安装完成，显示如图 7-39 所示的“安装结果”对话框。

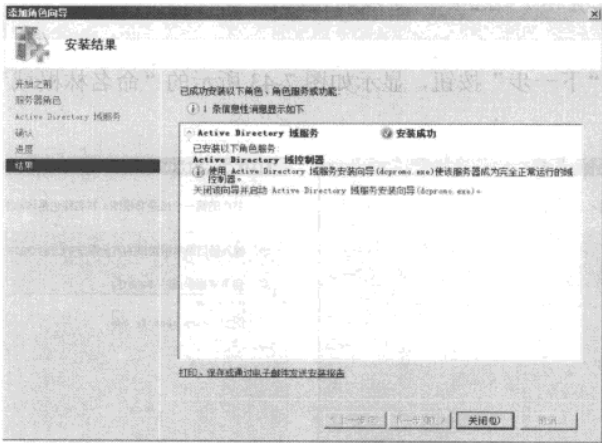


图 7-39 部署 AD DS 域服务之八

第 9 步，单击“关闭该向导并启动 Active Directory 域服务安装向导 (dcpromo.exe)”超链接，关闭“添加角色向导”对话框，启动“Active Directory 域服务安装向导”，显示如图 7-40 所示的“欢迎使用 Active Directory 域服务安装向导”对话框。

第 10 步，单击“下一步”按钮，显示如图 7-41 所示的“操作系统兼容性”对话框，显示操作系统兼容性信息。

第 11 步，单击“下一步”按钮，显示如图 7-42 所示的“选择某一部署配置”对话框。本例中，要安装全新的 Active Directory，选择“在新林中新建域”单选按钮。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

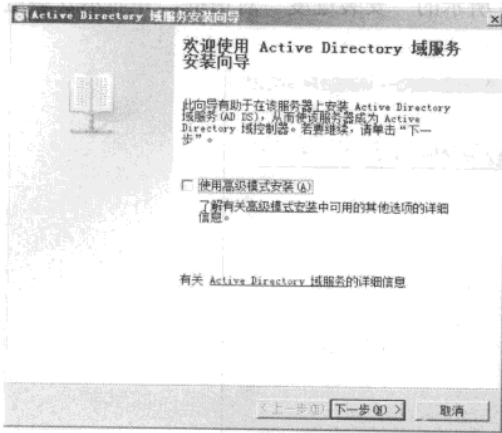


图 7-40 部署 AD DS 域服务之九

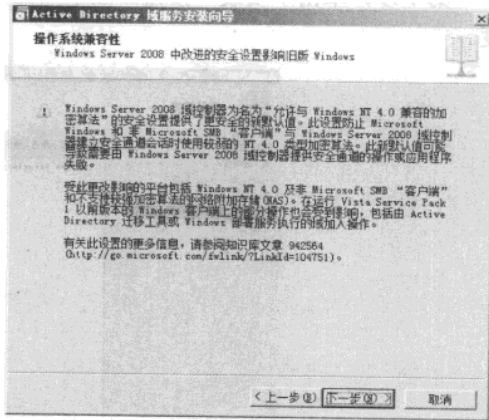


图 7-41 部署 AD DS 域服务之十

提示 “Active Directory 域服务安装向导”提供两种应用场景，一种为全新的 Active Directory（在新林中新建域），一种是在现有的 Active Directory 中添加域控制器（现有林）或者添加子域的情况。

第 12 步，单击“下一步”按钮，显示如图 7-43 所示的“命名林根域”对话框，设置新林的根域。

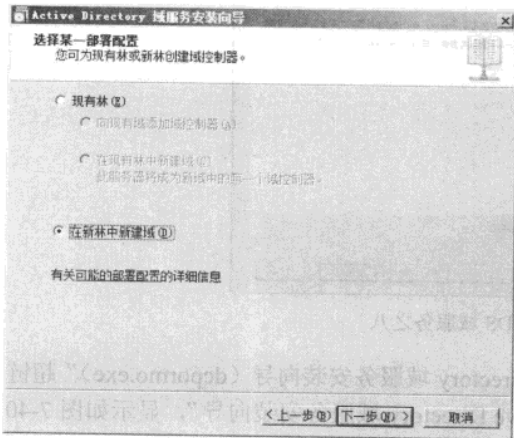


图 7-42 部署 AD DS 域服务之十一

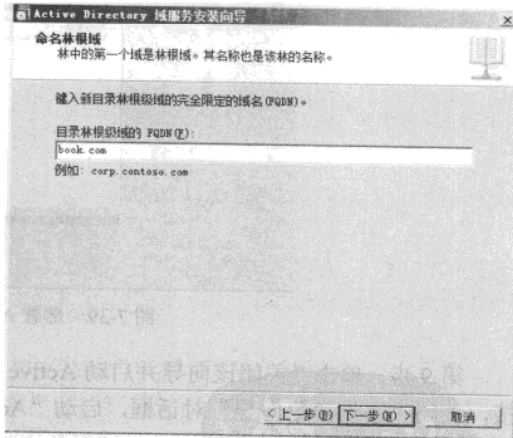


图 7-43 部署 AD DS 域服务之十二

第 13 步，单击“下一步”按钮，显示如图 7-44 所示的“设置林功能级别”对话框。安装向导提供 3 种模式，分别为 Windows 2000、Windows Server 2003 和 Windows Server 2008 模式。

提示

如果在网络环境中存在 Windows 2000 域控制器建议使用 Windows 2000 模式；如果既存在 Windows 2000 域控制器又存在 Windows Server 2003 域控制器或者只有 Windows Server 2003 域控制器，建议使用 Windows Server 2003 模式，Windows Server 2003 模式将包含 Windows 2000 的功能；如果全部是 Windows Server 2008 域控制器，建议选择 Windows Server 2008 模式。本例中设置域控制器的“林功能级别”为“Windows Server 2008”选项。如果选择林功能级别为 Windows Server 2008，则域功能级别默认设置为 Windows Server 2008 功能级别。在“Active Directory 域服务安装向导”中，将不显示域功能级别设置对话框。

第 14 步，单击“下一步”按钮，显示如图 7-45 所示的“其他域控制器选项”对话框。默认将域控制器设置为 DNS 服务器，如果网络中使用单独的 DNS 服务器，建议取消“DNS 服务器”复选框。本例中选择“DNS 服务器”复选框。

提示

在企业内部网络中，建议使用 Active Directory 集成区域 DNS 服务器，DNS 数据库中的内容将保存在 Active Directory 数据库中。如果企业内的计算机数量很多，建议创建独立的 DNS 服务器。

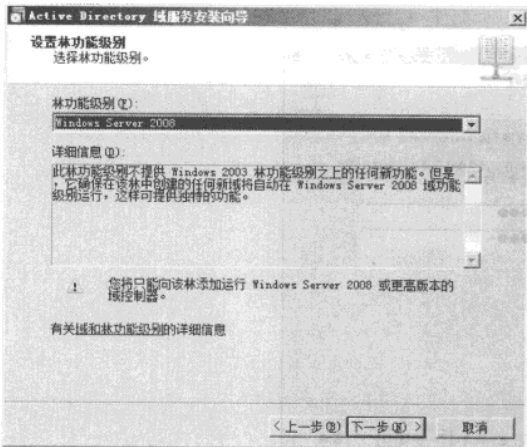


图 7-44 部署 AD DS 域服务之十三

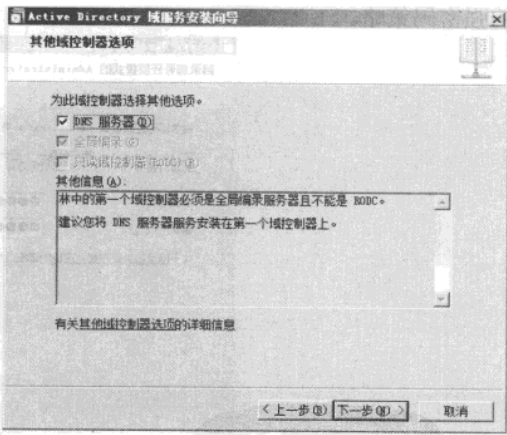


图 7-45 部署 AD DS 域服务之十四

第 15 步，单击“下一步”按钮，显示如图 7-46 所示的“Active Directory 域服务安装向导”对话框。提示管理员无法实现委派功能，该 DNS 服务器是网络中的第一台 DNS 服务器。

第 16 步，单击“是”按钮，显示如图 7-47 所示的“数据库、日志文件和 SYSVOL 的位置”对话框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

提示 Active Directory 数据库文件、日志文件和 SYSVOL 文件默认存储在“C:\Windows\NTDS”文件夹中，建议将 3 个文件分开存储，同时建议将上述文件存储在 RAID5 的磁盘阵列或者存储设备中。

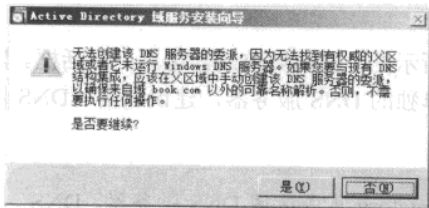


图 7-46 部署 AD DS 域服务之十五

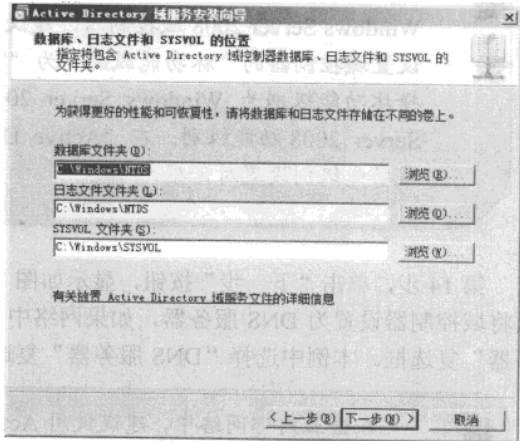


图 7-47 部署 AD DS 域服务之十六

第 17 步，单击“下一步”按钮，显示如图 7-48 所示的“目录服务还原模式的 Administrator 密码”对话框。设置目录还原模式下管理员的密码。该密码设置必须符合 Windows Server 2008 的强密码策略。

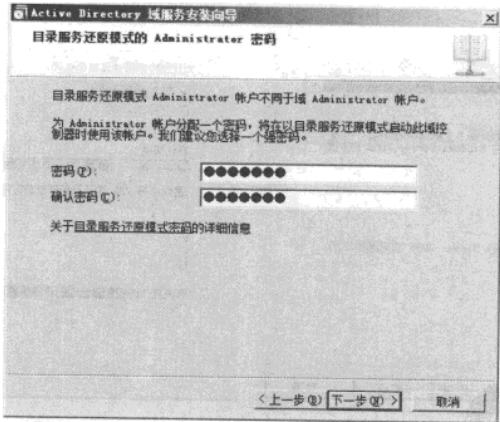


图 7-48 部署 AD DS 域服务之十七

提示 “目录服务还原模式”在 AD DS 域服务出现故障的情况下使用，该模式下需要密码控制，该密码不同于管理员账户的密码，且目录服务还原密码必须符合强密码策略设置原则。如果管理员忘记目录服务还原密码，可以使用“Ntdsutl”工具，重新设置该密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 18 步，单击“下一步”按钮，显示如图 7-49 所示的“摘要”对话框，显示 Active Directory 设置信息。

提示

单击该对话框中的“导出设置”按钮，可以将“Active Directory 域服务安装向导”设置过程中输入的参数导出并保存成文本文件，在安装 Server Core 模式的 AD DS 域服务时，使用导出的文本文件配置 AD DS 域服务。

第 19 步，单击“下一步”按钮，开始安装 AD DS 域服务，如图 7-50 所示。

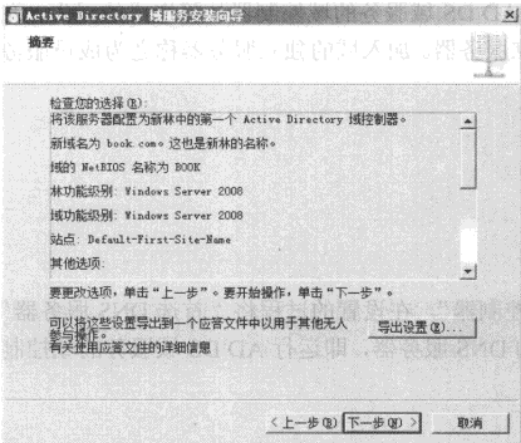


图 7-49 部署 AD DS 域服务之十八

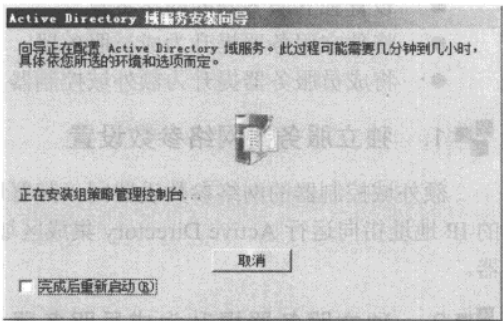


图 7-50 部署 AD DS 域服务之十九

第 20 步，安装完成后，显示如图 7-51 所示的“完成 Active Directory 域服务安装向导”对话框。

第 21 步，单击“完成”按钮，关闭“完成 Active Directory 域服务安装向导”，显示如图 7-52 所示的“Active Directory 域服务安装向导”对话框，提示重新启动计算机。

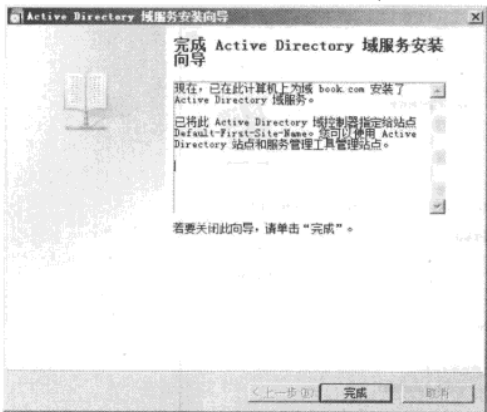


图 7-51 部署 AD DS 域服务之二十



图 7-52 部署 AD DS 域服务之二十一

网管天下 网管经验谈

第 22 步，单击“立即重新启动”按钮，重新启动计算机，成功安装 AD DS 域服务。

7.4.3 额外域控制器

在企业中，仅有一台 Active Directory 域控制器不能保证 AD DS 域服务的安全运行，如果运行 AD DS 域服务的服务器出现故障，整个企业将出现所有客户端计算机不能登录的情况，为了防止这种情况的发生，可以为运行 AD DS 域服务的域控制器创建一个与域控制器并行的域控制器，即额外域控制器。在运行 AD DS 域服务的域控制器出现故障的情况下，额外域控制器接管 Active Directory 工作，避免因运行 AD DS 域服务的域控制器故障造成的损失。在没有部署额外域控制器前，该服务器称之为独立服务器。加入域的独立服务器称之为成员服务器。部署额外域控制器的过程分为以下部分：

- 设置独立服务器的网络参数。
- 将独立服务器提升为成员服务器。
- 将成员服务器提升为额外域控制器。

1. 独立服务器网络参数设置

额外域控制器的网络参数设置同“部署域控制器”，在设置的过程将“首选 DNS 服务器”的 IP 地址指向运行 Active Directory 集成区域的 DNS 服务器，即运行 AD DS 域服务的域控制器。

2. 独立服务器提升为成员服务器

将独立服务器加入到 Active Directory 中，加入到 Active Directory 的服务器称之为“成员服务器”。

第 1 步，以本地管理员的账户登录独立服务器，右击“开始”→“计算机”选项，在弹出的快捷菜单中选择“属性”命令，显示如图 7-53 所示的“系统”窗口。

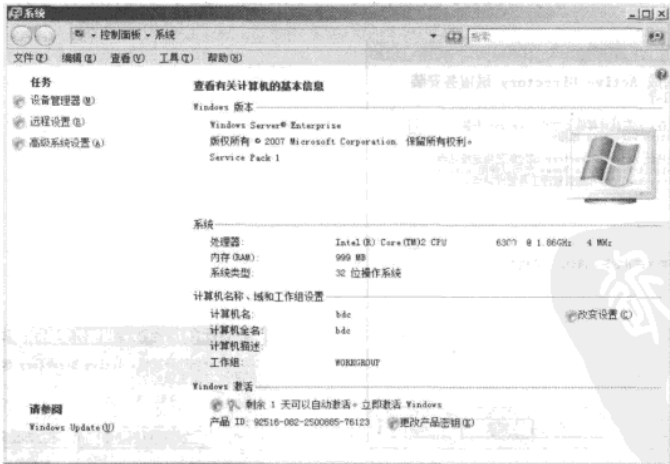


图 7-53 独立服务器提升为成员服务器之一

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 2 步，在“任务”面板中，单击“高级系统设置”超链接，显示如图 7-54 所示的“系统属性”对话框。

第 3 步，切换到“计算机名”选项卡，显示如图 7-55 所示对话框。

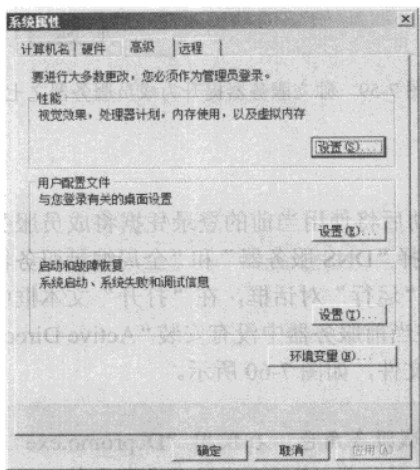


图 7-54 独立服务器提升为成员服务器之二

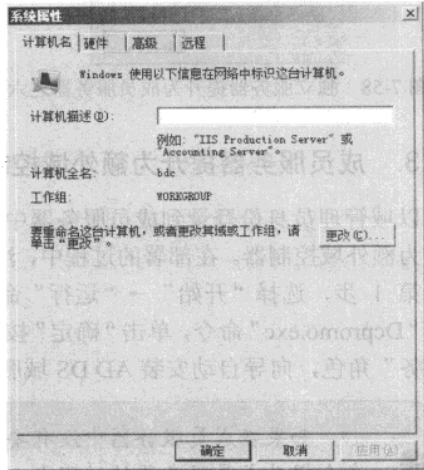


图 7-55 独立服务器提升为成员服务器之三

第 4 步，单击“更改”按钮，显示如图 7-56 所示的“计算机名/域更改”对话框。在“隶属于”分组区域中，选择“域”单选按钮，在“域”文本框中，输入目标域的名称，如图 7-56 所示。

第 5 步，单击“确定”按钮，显示如图 7-57 所示的“Windows 安全”对话框。输入具备将用户加入域的用户名称和密码。

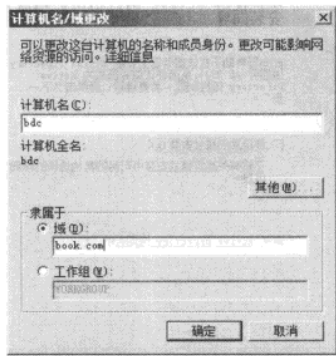


图 7-56 独立服务器提升为成员服务器之四

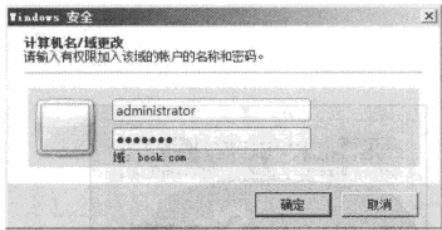


图 7-57 独立服务器提升为成员服务器之五

第 6 步，单击“确定”按钮，显示如图 7-58 所示的“计算机名/域更改”对话框。

第 7 步，单击“确定”按钮，显示如图 7-59 所示的“计算机名/域更改”对话框，提示管理员需要重新启动服务器。

第 8 步，单击“确定”按钮，重新启动服务器，并以域管理员身份登录。

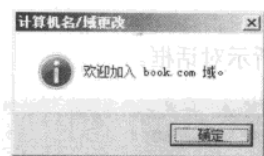


图 7-58 独立服务器提升为成员服务器之六

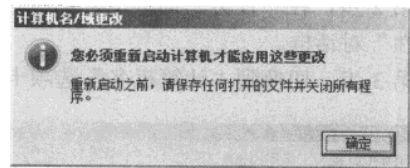


图 7-59 独立服务器提升为成员服务器之七

3. 成员服务器提升为额外域控制器

以域管理员身份登录到成员服务器中，成功启动后将使用当前的登录凭据将成员服务器提升为额外域控制器。在部署的过程中，注意是否选择“DNS 服务器”和“全局编录服务器”。

第 1 步，选择“开始”→“运行”命令，显示“运行”对话框，在“打开”文本框中，输入“Dcpromo.exe”命令，单击“确定”按钮，如果在当前服务器中没有安装“Active Directory 域服务”角色，向导自动安装 AD DS 域服务需要的文件，如图 7-60 所示。

提示

如果在成员服务器中没有安装 AD DS 域服务角色，在使用“Dcpromo.exe”命令提升成员服务器的过程中，将在后台自动加载 AD DS 域服务角色文件。换句话说，在部署域控制器或者额外域控制器的过程中，可以不安装 AD DS 域服务角色。

第 2 步，AD DS 域服务需要的文件加载完成后，显示如图 7-61 所示的“欢迎使用 Active Directory 域服务安装向导”对话框。



图 7-60 提升域额外控制器之一

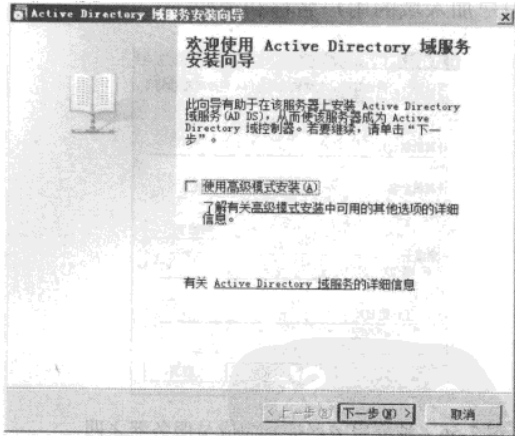


图 7-61 提升域额外控制器之二

第 3 步，单击“下一步”按钮，显示如图 7-62 所示的“操作系统兼容性”对话框，提示管理员关于系统兼容方面的信息。

第 4 步，单击“下一步”按钮，显示如图 7-63 所示的“选择某一部署配置”对话框。本例将安装 Book.com 域的额外域控制器，选择“现有林”下的“向现有域添加域控制器”单选

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按钮。

提示

选择“向现有域添加域控制器”单选按钮，将提升成员服务器为额外域控制器。选择“在现有林中新建域”单选按钮，在当前域中创建新的子域。

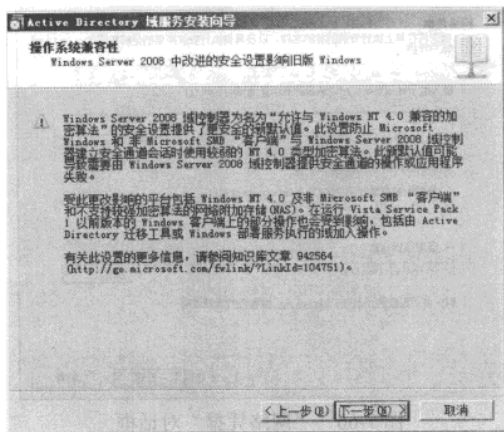


图 7-62 提升域额外控制器之三

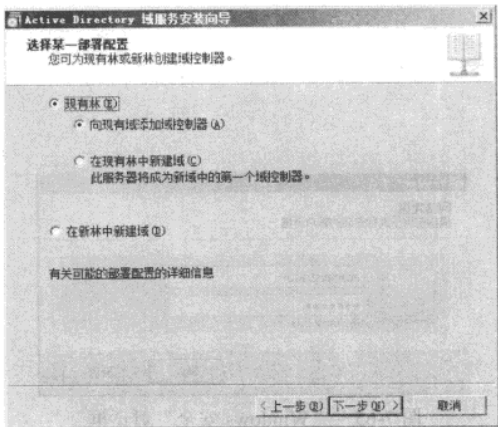


图 7-63 提升域额外控制器之四

第 5 步，单击“下一步”按钮，显示如图 7-64 所示的“网络凭据”对话框，设置具备将用户添加到 Active Directory 中的账户名称，使用默认值即可。

提示

提升额外域控制器建议使用域管理员，在登录成员服务器时也使用域管理员，“Active Directory 域服务安装向导”自动将登录的用户作为安装凭据。

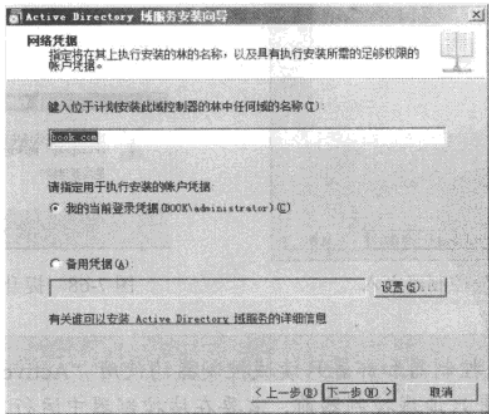


图 7-64 提升域额外控制器之五

网管天下 网管经验谈

- ① 在“输入位于计划安装此域控制器的林中任何域的名称”文本框中，输入已经安装的 Active Directory 名称。
- ② 如果使用其他账户，则单击“设置”按钮，显示如图 7-65 所示的“Windows 安全”对话框，输入 book.com 域中管理员的用户名和密码。
- ③ 单击“确定”按钮，关闭“Windows 安全”对话框，返回到“网络凭据”对话框，如图 7-66 所示。

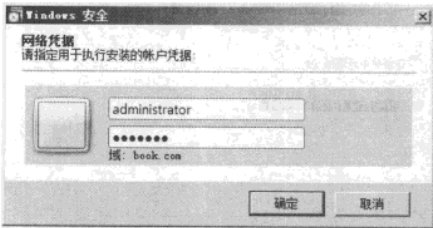


图 7-65 “Windows 安全”对话框

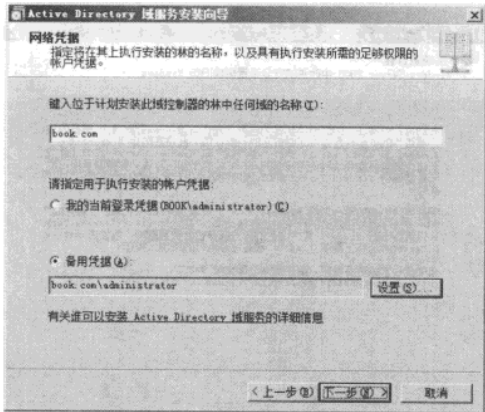


图 7-66 “网络凭据”对话框

第 6 步，单击“下一步”按钮，显示如图 7-67 所示的“选择一个域”对话框。向导自动检索设置的 Active Directory 中可用的域，选择目标域。

第 7 步，单击“下一步”按钮，显示如图 7-68 所示的“Active Directory 域服务安装向导”对话框，提示无法安装只读域控制器。

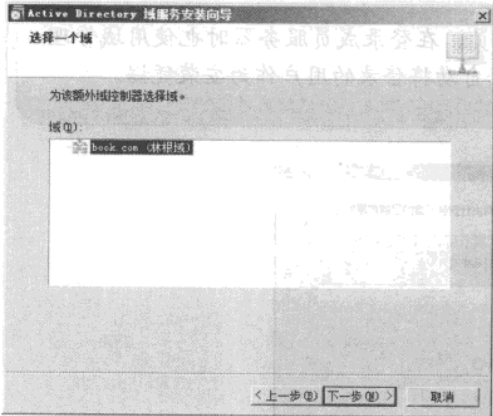


图 7-67 提升域额外控制器之六

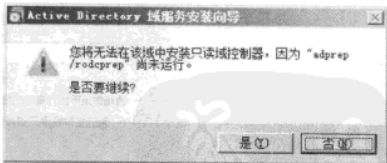


图 7-68 提升域额外控制器之七

提示 部署额外域控制器和部署只读域控制器均使用“Active Directory 域服务安装向导”，在部署只读域控制器前，需要在域控制器中运行准备 RODC 脚本，成功后方能在基于 Windows Server 2008 AD DS 域服务的林中部署只读域控制器。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

高可用性应用 | 7

第 8 步，单击“下一步”按钮，显示如图 7-69 所示的“请选择一个站点”对话框。为额外域控制器选择一个站点，在本例中使用默认站点且只有一个站点，选择默认站点即可。

第 9 步，单击“下一步”按钮，显示如图 7-70 所示的“其他域控制器选项”对话框。根据需要选择“DNS 服务器”和“全局编录”复选框。

提示 如果部署目标为“只读域控制器”，建议不要选择“全局编录”复选框。如果部署额外域控制器，建议选择“DNS 服务器”复选框。根据网络规划确认是否将额外域控制器提升为“全局编录”服务器。在域控制器部署完成后，可以使用“Active Directory 站点和服务”将选择的额外域控制器提升为“全局编录”服务器。

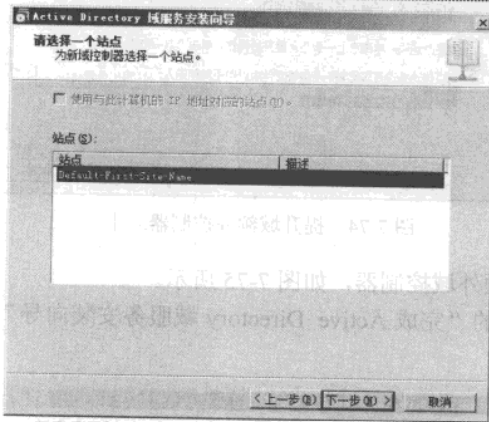


图 7-69 提升域额外控制器之八

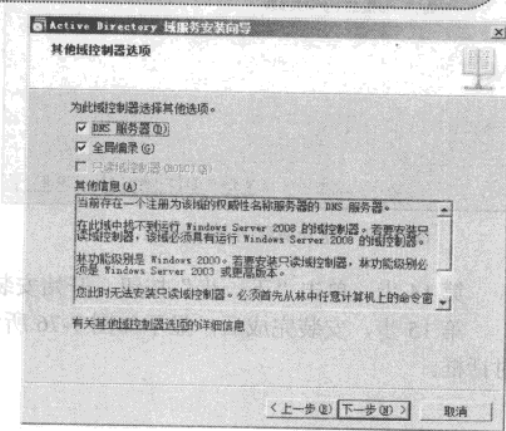


图 7-70 提升域额外控制器之九

第 10 步，单击“下一步”按钮，显示如图 7-71 所示的对话框，提示 DNS 委派信息。

第 11 步，单击“下一步”按钮，显示如图 7-72 所示的“数据库、日志文件和 SYSVOL 的位置”对话框。建议将数据库、日志文件和 SYSVOL 文件夹分别存储在不同的物理磁盘上。

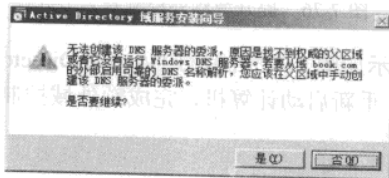


图 7-71 提升域额外控制器之十

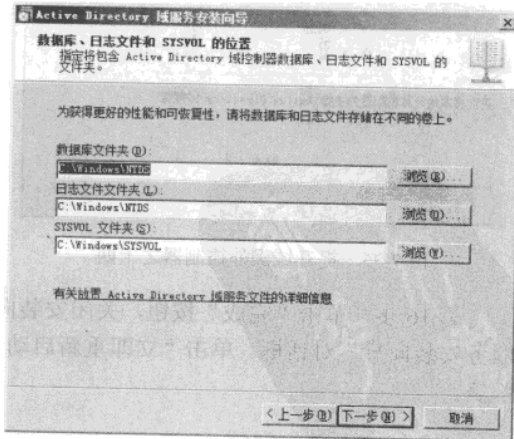


图 7-72 提升域额外控制器之十一

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 12 步，单击“下一步”按钮，显示如图 7-73 所示的“目录服务还原模式的 Administrator 密码”对话框。目录服务还原密码必须符合“强密码”策略原则。

第 13 步，单击“下一步”按钮，显示如图 7-74 所示的“摘要”对话框，显示 Active Directory 设置信息。

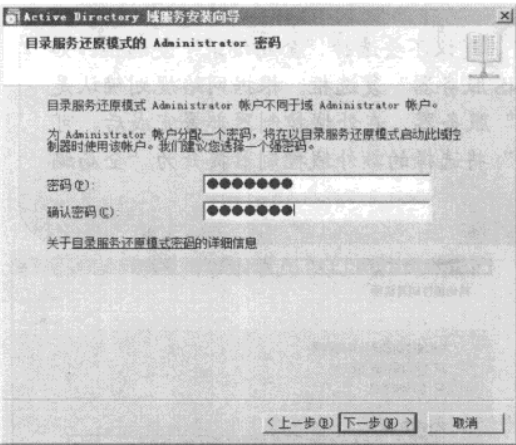


图 7-73 提升域额外控制器之十二

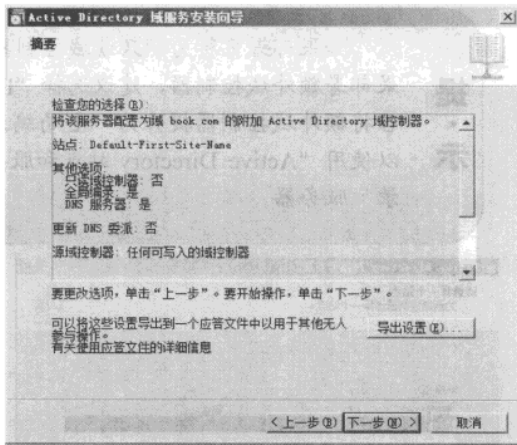


图 7-74 提升域额外控制器之十三

第 14 步，单击“下一步”按钮，开始安装额外域控制器，如图 7-75 所示。
第 15 步，安装完成后，显示如图 7-76 所示的“完成 Active Directory 域服务安装向导”对话框。

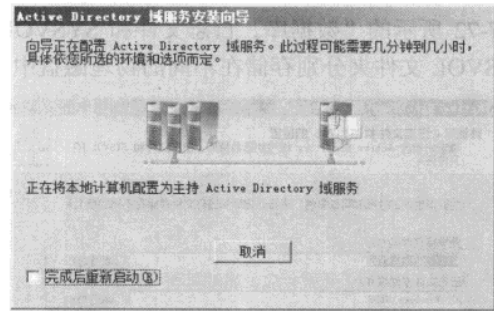


图 7-75 提升域额外控制器之十四

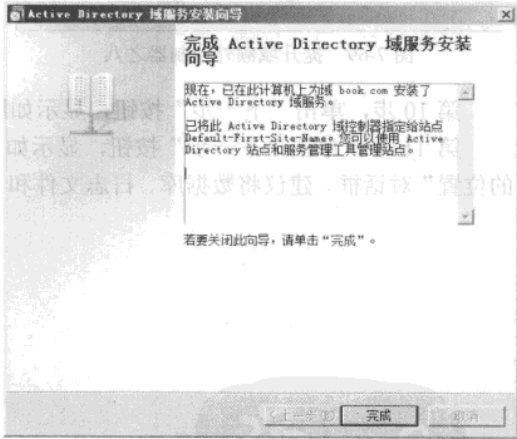


图 7-76 提升域额外控制器之十五

第 16 步，单击“完成”按钮，关闭安装向导，显示如图 7-77 所示的“Active Directory 域服务安装向导”对话框。单击“立即重新启动”按钮，重新启动计算机，完成额外域控制器的部署。

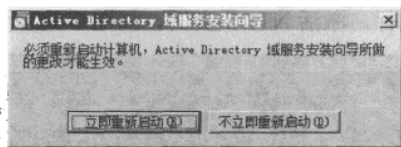


图 7-77 提升域额外控制器之十六

7.4.4 | 管理域控制器

AD DS 域服务后台是 Active Directory 数据库，既然是数据库就需要管理。在 AD DS 域服务运行时，将不能维护 Active Directory 数据库，只有在停止 AD DS 域服务之后才能维护 Active Directory 数据库。停止 AD DS 域服务的方法有多种，可以在“服务”管理控制台中停止，也可以使用“net”命令停止，或者使用目录还原模式维护 Active Directory 数据库。

1. 移动 Active Directory 数据库文件

Active Directory 数据库的默认位置是“c:\windows\ntds”目录，如果在部署 AD DS 初期计划分配的磁盘空间不足，或者担心 Active Directory 数据库安全，可以将其重定向到其他磁盘或者文件夹中。重定向 Active Directory 数据库需要停止 AD DS 服务。

第 1 步，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，打开“命令提示符”窗口。

第 2 步，在命令提示符下，输入如下命令：

```
net stop ntds
```

按 Enter 键，命令成功执行，停止 AD DS 域服务，如图 7-78 所示。



图 7-78 重定向 Active Directory 数据库之一

第 3 步，在命令提示符下，输入如下命令：ntdsutil

在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil :Activate Instance NTDS
```

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

按 Enter 键，命令成功执行，激活 NTDS 实例，如图 7-79 所示。



图 7-79 重定向 Active Directory 数据库之二

第 4 步，在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil :Files
```

按 Enter 键，命令成功执行。

第 5 步，在 file maintenance 命令提示符下，输入以下命令：

```
file maintenance :info
```

按 Enter 键，命令成功执行，显示 Active Directory 数据库的基本信息，如图 7-80 所示。



图 7-80 重定向 Active Directory 数据库之三

第 6 步，在 file maintenance 命令提示符下，输入以下命令：

```
file maintenance :move db to c:\ntds
```

按 Enter 键，将 Active Directory 数据库移动到 “c:\ntds” 目录下，如图 7-81 所示。



图 7-81 重定向 Active Directory 数据库之四

第 7 步，在 file maintenance 命令提示符下，输入以下命令：

```
file maintenance :info
```

按 Enter 键，命令成功执行，显示 Active Directory 数据库的基本信息，如图 7-82 所示。



图 7-82 重定向 Active Directory 数据库之五

从图中可以看出，Active Directory 数据库文件已经由默认安装位置重定向到“c:\ntds”目录下。

第 8 步，输入两次“quit”命令，退出 ntdsutil 命令，重新启动 AD DS 服务即可。

2. 收缩 Active Directory 数据库文件

Active Directory 数据库分为离线整理和在线整理，在线整理由 AD DS 域服务自动完成，离线整理需要管理员停止 AD DS 域服务后，手动执行 Active Directory 数据库整理。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 1 步，在命令提示符下，输入如下命令，停止 AD DS 域服务。

```
net stop NTDS
```

按 Enter 键，命令成功执行，停止 AD DS 域服务。

第 2 步，在命令提示符下，输入如下命令：

```
ntdsutil
```

在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil :Activate Instance NTDS
```

按 Enter 键，命令成功执行，激活 NTDS 实例。

第 3 步，在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil Files
```

第 4 步，在 file maintenance 命令提示符下，输入以下命令：

```
file maintenance :compact to c:\temp
```

按 Enter 键，命令成功执行，压缩并整理当前的 Active Directory 数据库，如图 7-83 所示。



图 7-83 离线整理 Active Directory 数据库之一

第 5 步，输入两次“quit”命令，退出 ntdsutil 命令。

第 6 步，在“MSDOS”命令提示符下，输入如下命令：

```
copy "c:\temp\ntds.dit" "c:\ntds\ntds.dit"
```

使用压缩过的 Active Directory 数据库文件，覆盖默认位置的 Active Directory 数据库文件，如图 7-84 所示。



图 7-84 离线整理 Active Directory 数据库之二

第 7 步，在“MSDOS”命令提示符下，输入命令：

```
del c:\ntds\*.log
```

删除默认 Active Directory 数据库目录下的日志文件，如图 7-85 所示。



图 7-85 离线整理 Active Directory 数据库之三

第 8 步，在命令行提示符下，输入：

```
net start NTDS
```

按 Enter 键，命令成功执行，重新启动 AD DS 域服务。

3. 清理域控制器元数据

在 Active Directory 数据库中，由于硬件损坏或者非正规操作 Active Directory 数据库，将在 Active Directory 数据库中遗留“垃圾”数据，当此类数据在域控制器之间复制时，将产生

网管天下 网管经验谈

错误信息。因此，清理 Active Directory 中失效的元数据，是在域控制器等错误发生时必须的工作。

本例模拟一台额外域控制器突然损坏的状况，从 Active Directory 数据库中删除损坏的域控制器信息。

第 1 步，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，打开“命令提示符”窗口。在命令提示符下，输入如下命令：

```
ntdsutil
```

按 Enter 键，命令成功执行，切换到 ntdsutil 命令提示符。

第 2 步，在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil: metadata cleanup
```

按 Enter 键，命令成功执行，切换到 metadata cleanup 命令提示符。

在 metadata cleanup 命令提示符下，输入如下命令：

```
metadata cleanup: select operation target
```

按 Enter 键，命令成功执行，切换到 select operation target 命令提示符，如图 7-86 所示。



图 7-86 清理元数据之二

第 3 步，在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: connections
```

按 Enter 键，命令成功执行，切换到 server connections 命令提示符。

在 server connections 命令提示符下，输入如下命令：

```
metadata cleanup: connect to server dc.book.com
```

按 Enter 键，命令成功执行，连接到域控制器 dc.book.com 中。

提
·
示

dc.book.com 是域控制器的 DNS 名称，用主机名或 FQDN 均可。建议使用 FQDN 名称。注意，虽然帮助文件中说明可以使用 IP 链接，实际上发现用 IP 连接，将出现参数不正确的出错提示。在这里要连接的域控制器，是一个正常工作的、可操作的域控制器，而不是要清理的目标域控制器对象。

在 server connections 命令提示符下，输入如下命令：

```
metadata cleanup: quit
```

按 Enter 键，命令成功执行，返回到上级目录，如图 7-87 所示。



图 7-87 清理元数据之三

第 4 步，在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: list site
```

按 Enter 键，命令成功执行，列出所有可用的站点。

在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: select site 0
```

按 Enter 键，命令成功执行，选择站点，如图 7-88 所示。数字 0 是故障域控制器所在的站点的索引号。

第 5 步，在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: list domains
```

按 Enter 键，命令成功执行，列出所有可用域。

在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: select domain 0
```


网管天下 网管经验谈



图 7-88 清理元数据之四

按 Enter 键，命令成功执行，选择域控制器所在的域，如图 7-89 所示。数字 0 是故障域控制器所在的域的索引号。



图 7-89 清理元数据之五

第 6 步，在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: list servers for domain in site
```

按 Enter 键，命令成功执行，列出选择的域中所有的域控制器，包括正常的和出现故障的域控制器。

在 select operation target 命令提示符下，输入如下命令：

```
metadata cleanup: select server 1
```

按 Enter 键，命令成功执行，选择需要清理的目标域控制器，数字 0 是故障域控制器的索引号。

在 `select operation target` 命令提示符下，输入如下命令：

```
metadata cleanup: quit
```

按 Enter 键，命令成功执行，返回到上级目录的 `metadata cleanup` 命令提示符，如图 7-90 所示。

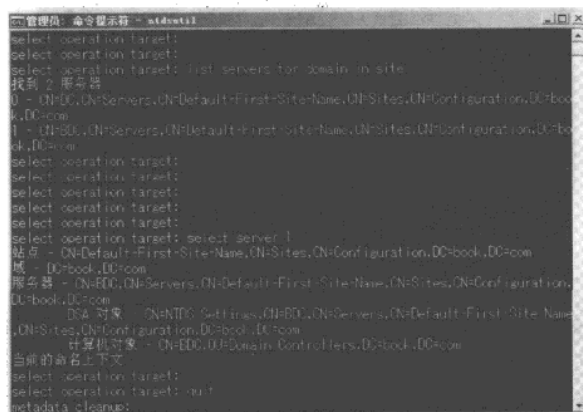


图 7-90 清理元数据之六

第 7 步，在 `metadata cleanup` 命令提示符下，输入如下命令：

```
metadata cleanup: remove select server
```

按 Enter 键，命令成功执行，显示如图 7-91 所示的“服务器删除确认对话框”。



图 7-91 清理元数据之七

第 8 步，单击“是”按钮，执行故障域控制器元数据清理过程，清理完成显示如图 7-92 所示信息，清理成功。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-92 清理元数据之八

提·示

在实际操作中，必须先做元数据清理，然后再到管理工具中删除相应的对象。若是直接到管理工具中去删除，系统将不允许删除。

如果清理的是 Server 对象，元数据清理完成后，需要完成以下操作。

- ① 打开“Active Directory 站点和服务”，展开适当站点，删除相应 Server 对象。
- ② 打开“Active Directory 用户和计算机”，打开 Domain Controllers 组织单位，删除相应的域控制器对象。
- ③ 如果清理的是 Domain 对象，元数据清理完成后，需要完成以下操作。
- ④ 打开“Active Directory 域和信任关系”，删除相应的已经无效信任关系。否则该域名将出现登录的域列表中。

4. 设置“目录服务还原模式”密码

在 Active Directory 管理控制台 (Active Directory 用户和计算机、Active Directory 域和信任关系, 以及 Active Directory 站点和服务) 中, 不能重命名目录还原模式密码。如果管理员遗忘该密码, 可以在 “ntdsutil” 中重置该密码。

第1步,选择“开始”→“所有程序”→“附件”→“命令提示符”选项,显示如图3-58所示的“命令提示符”窗口。在命令提示符下,输入如下命令:

ntdsutil

按 Enter 键，命令成功执行，切换到 ntdsutil 命令提示符。

第2步，在 `ntdsutil` 命令提示符下，输入以下命令：

ntdsutil: Set DSRM Password

按 Enter 键，命令成功执行，切换到“重置 DSRM 管理员密码”命令提示符。

第3步，在“重置 DSRM 管理员密码”命令提示符下，输入以下命令：

```
ntdsutil: reset password on server dc.book.com
```

按 Enter 键，命令成功执行，提示“请输入 DS 还原模式 Administrator 账户的密码”，输入新的密码，该密码必须符合强密码策略。

按 Enter 键，再次确认密码。

按 Enter 键，密码设置成功，如图 7-93 所示。



图 7-93 重置目录服务还原模式管理员账户密码之二

5. 安全标识符清理

网络维护时，管理员为了节省时间，经常使用操作系统备份工具完整备份操作系统，当操作系统出现故障，管理员可以在极短的时间之内恢复操作系统，在这种情况下，由于恢复的操作系统使用的安全标识符（SID）和以前的操作系统相同，在 Active Directory 数据库中将出现重复的 SID，重名的计算机将不能登录到域中。

第1步，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，显示如图 3-58 所示的“命令提示符”窗口。在命令提示符下，输入如下命令：

```
ntdsutil
```

按 Enter 键，命令成功执行，切换到 ntdsutil 命令提示符。

第2步，在 ntdsutil 命令提示符下，输入以下命令：

```
ntdsutil: security account management
```

按 Enter 键，命令成功执行，切换到“安全策略账户维护”命令提示符，如图 7-94 所示。

第3步，在“安全策略账户维护”命令提示符下，输入以下命令：

```
安全策略账户维护: connect to server dc.book.com
```

按 Enter 键，命令成功执行，链接到目标域控制器。

网管天下

网管经验谈



图 7-94 安全标识符清理之二

在“安全策略账户维护”命令提示符下，输入以下命令：

```
安全策略账户维护: check duplicate sid
```

按 Enter 键，命令成功执行，检查当前 Active Directory 数据库中是否存在重复的 SID，结果输出在 dupsid.log 文件中，如图 7-95 所示。



图 7-95 安全标识符清理之三

第 4 步，在“安全策略账户维护”命令提示符下，输入以下命令：

```
安全策略账户维护: cleanup duplicate sid
```

按 Enter 键，命令成功执行，清除当前 Active Directory 数据库中重复的 SID，结果输出在 dupsid.log 文件中，如图 7-96 所示。

第 5 步，输入多次“quit”命令，退出“ntdsutil”工具。



图 7-96 安全标识符清理之四

7.4.5 AD DS 域服务故障

Windows Server 2008 部署的网络，由于病毒、使用或操作不当、安装添加/删除程序等原因；或者服务器的硬件故障，造成工作站在登录时也就是在进行身份验证时，登录速度缓慢；或者在域控制器上进行一些管理或维护性的操作时，速度过慢；或者由于以前安装配置的问题，在域控制器上安装新的应用软件时，导致不能进行安装。在这种情况下，就需要重新安装域控制器。

1. 故障描述

在基于 Windows Server 2008 网络中，如果其中一台工作站损坏，可以直接用一台全新的计算机替换，当使用这台工作站的用户进行登录时，数据会自动恢复。因为域控制器保存了大量的用户及与用户相关的信息和数据，这时候，只有在保存好用户数据及信息的前提下，才能重新安装。保存用户的数据可以直接备份到移动存储设备，如磁带机或者活动硬盘上。

在企业网络中，对服务器进行重新安装的同时，也不能影响网络的使用，而且使用重新安装的方法修复服务器。在安装后，也应该与安装之前的正常状态一样，用户不应该有所察觉。

(1) 域控制器出现故障，但仍然可用。

假设有故障的域控制器是计算机 A，原来额外域控制器为计算机 B（无故障），将计算机 B 升级为新域控制器（此时 A 将自动降级成额外域控制器），然后在原域控制器（计算机 A）上运行 `dcpromo` 命令将其本身从 Active Directory 中降级为成员服务器，将成员服务器降级为独立服务器后，在 Active Directory 数据库中清理原数据即可删除原域控制器。

原域控制器（计算机 A）故障恢复后，重新格式化硬盘、重新安装 Windows Server 2008，并升级成新域控制器（计算机 B）的额外域控制器，然后再将 A 升级成域控制器，在整个恢复的过程中，只要 Active Directory 数据库完好，所有的用户信息将同步迁移。

(2) 域控制器已经彻底损坏并且不能恢复时，整个网络不能正常使用。

将额外域控制器升级成域控制器，同时转移操作主机角色。操作主机角色分为 5 个部分：RID 主机角色、PDC 模拟器角色、结构主机角色、域命名操作主机角色和架构主机角色。在正常的情况下，如果域控制器和额外域控制器均可操作，可以“转移”主机角色；如果域控制

网管天下 网管经验谈

器已经损坏并且不可修复，就要强制“占用”主机角色。

2. 域控制器故障但仍然可用

当管理员发现出现“域控制器故障但仍然可用”错误时，按照下列步骤将额外域控制器提升为域控制器，重新安装原域控制器，将原域控制器作为额外域控制器使用或者重新提升为域控制器。本节中举例说明，怎样将一台出现故障的域控制器迁移额外域控制器，原来的额外域控制器升级为新的域控制器。

(1) 提升额外域控制器为全局编录服务器。

在将额外域控制器提升为域控制器前，首先将额外域控制器提升为“全局编录”服务器，提升过程在“Active Directory 站点和服务”控制台中完成。

第 1 步，以域管理员身份登录到额外域控制器，选择“开始”→“管理工具”→“Active Directory 站点和服务”选项，显示如图 7-97 所示的“Active Directory 站点和服务”窗口。

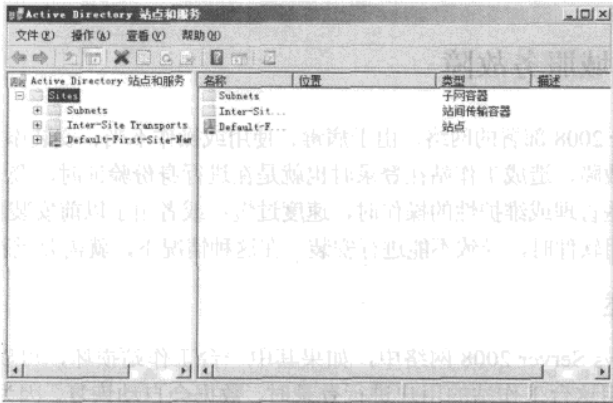


图 7-97 提升额外域控制器为全局编录服务器之一

第 2 步，选择“Sites”→“Default-First-Site-Name”→“Servers”→“BDC”选项，如图 7-98 所示。

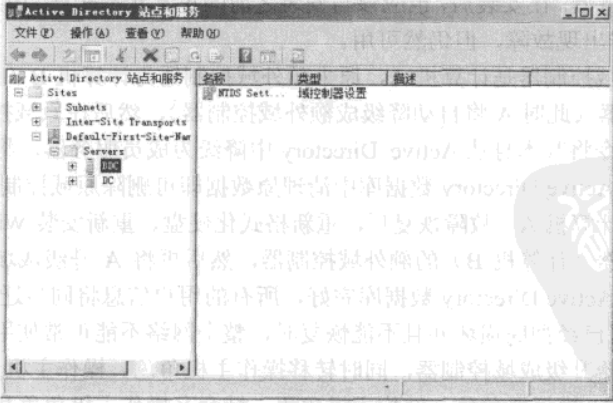


图 7-98 提升额外域控制器为全局编录服务器之二

第 3 步，在窗口中部区域，右击“NTDS Settings”选项，在弹出的快捷菜单中选择“属

性”命令，显示如图 7-99 所示的“NTDS Settings 属性”对话框。

第 4 步，在弹出的“NTDS Settings 属性”中，在“查询策略”下拉列表框中选择“Default Query Policy”选项，并选中“全局编录”复选框，如图 7-100 所示。

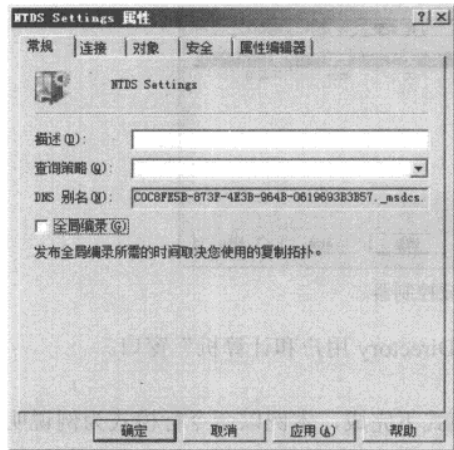


图 7-99 提升额外域控制器为全局编录服务器之三

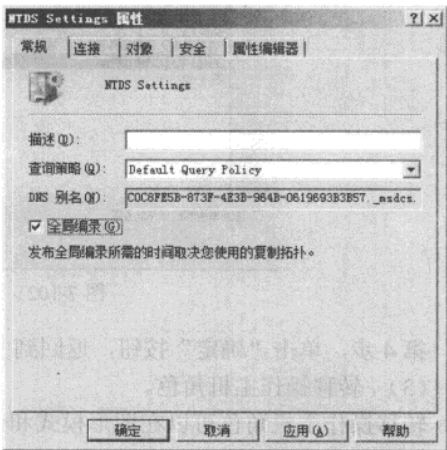


图 7-100 提升额外域控制器为全局编录服务器之四

第 5 步，单击“确定”按钮，返回“Active Directory 站点和服务”窗口。

(2) 连接额外域控制器。

本实例的前提是域控制器可用，在域控制器中可用连接到额外域控制器。

第 1 步，以域管理员身份登录到域控制器中，选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，显示如图 7-101 所示的“Active Directory 用户和计算机”窗口。

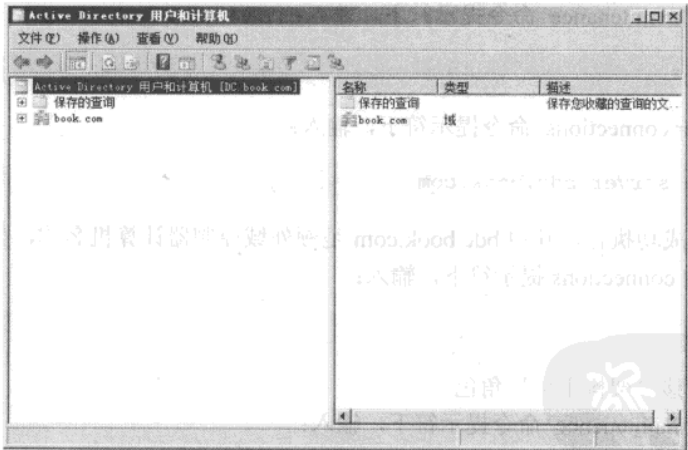


图 7-101 连接额外域控制器之一

第 2 步，右击“Active Directory 用户和计算机”选项，在弹出的快捷菜单中选择“更改域控制器”命令，显示如图 7-102 所示的“更改目录服务器”对话框。

第 3 步，选择“此域控制器或 AD LDS 实例”单选按钮，在可用的域控制器列表框中，选择额外域控制器，本例中选择“bdc.book.com”选项。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

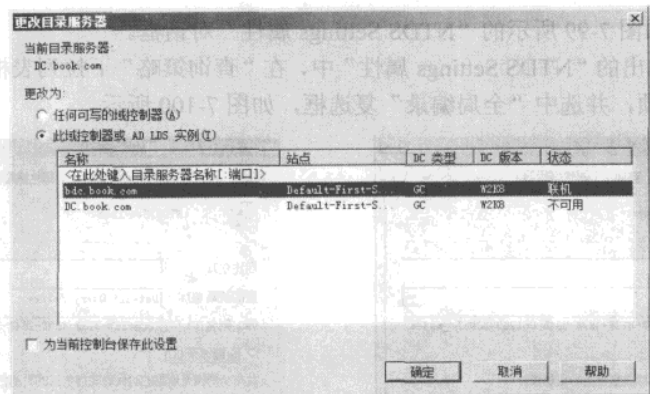


图 7-102 连接额外域控制器二

第 4 步，单击“确定”按钮，返回到“Active Directory 用户和计算机”窗口。

(3) 转移操作主机角色。

转移操作主机角色可以在图形模式和命令行模式下完成，本例以命令行模式为例说明操作主机角色的转移方法。

第 1 步，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，打开“命令提示符”窗口。

第 2 步，在命令提示符下，输入如下命令：ntdsutil

① 在 ntdsutil 命令提示符下，输入：

```
roles
```

② 在 fsmo maintenance 命令提示符下，输入：

```
connections
```

③ 在 server connections 命令提示符下，输入：

```
connect to server bdc.book.com
```

命令行成功执行，其中 bdc.book.com 是额外域控制器计算机名称，如图 7-103 所示。

④ 在 server connections 提示符下，输入：

```
Quit
```

第 3 步，转移“架构主机”角色。

① 在 fsmo maintenance 命令提示符下，输入：

```
Transfer schema master
```

② 显示如图 7-104 所示的“角色传送确认对话”对话框，提示管理员是否需要将架构主机角色传送到目标服务器中。

③ 单击“是”按钮，将架构主机角色传送到额外域控制器中，如图 7-105 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

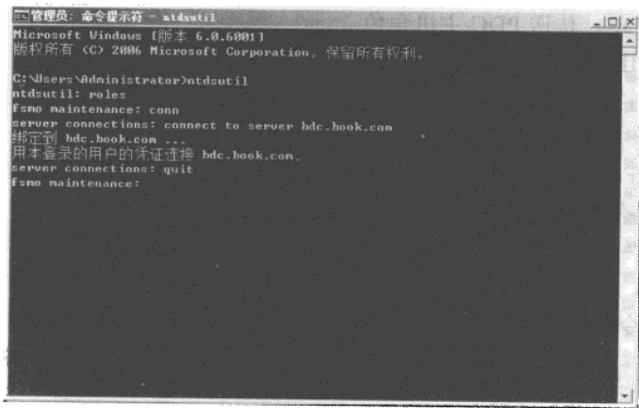


图 7-103 转移架构主机角色之一



图 7-104 转移架构主机角色之二



图 7-105 转移架构主机角色之三

- 第 4 步，在 fsmo maintenance 命令提示符下，分别输入：
- Transfer infrastructure master，传送结构主机角色。
 - Transfer naming master，传送域命名主机角色。

网管天下 网管经验谈

- Transfer PDC，传送 PDC 主机角色。
- Transfer RID master，传送 RID 主机角色。

将传送不同的主机角色。

(4) 查看操作主机角色。

Windows Server 2008 安装完成后，默认已经安装 netdom 命令，管理员使用该工具可以查看操作主机角色部署哪一台域控制器中。

第 1 步，选择“开始”→“运行”命令，显示“运行”对话框，在文本框中，输入“cmd”，单击“确定”按钮，打开的“命令提示符”窗口。

第 2 步，在命令行提示符下，输入如下命令：

```
netdom query fsmo
```

按 Enter 键，命令成执行，显示操作主机角色所在的域控制器，如图 7-106 所示。



图 7-106 命令行模式看操作主机角色

(5) 原域控制器降级为成员服务器。

原域控制器自动降级为额外域控制器，使用“dcpromo.exe”命令，将额外域控制器降级为成员服务器。

第 1 步，以管理员身份登录到原域控制器，选择“开始”→“运行”命令，显示“运行”对话框，在文本框中，输入“dcpromo.exe”，单击“确定”按钮，显示如图 7-107 所示的“欢迎使用 Active Directory 域服务安装向导”对话框。

第 2 步，单击“下一步”按钮，显示如图 7-108 所示的“Active Directory 域服务安装向导”对话框。

第 3 步，单击“确定”按钮，显示如图 7-109 所示的“删除域”对话框。取消“删除该域，因为此服务器是该域中的最后一个域控制器”复选框。

提示 如果需要删除的域控制器是网络中的最后一个域控制器，删除后网络中将没有域控制器，选择“删除该域，因为此服务器是该域中的最后一个域控制器”复选框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

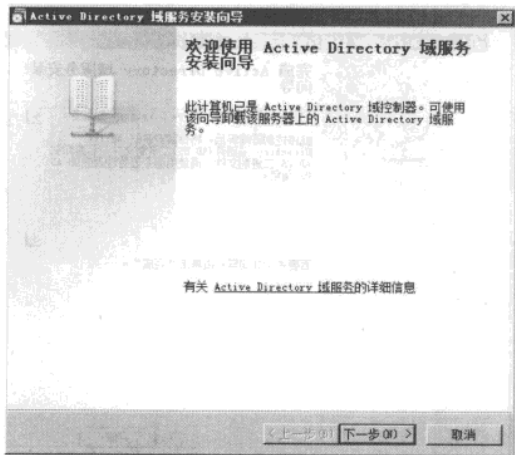


图 7-107 原域控制器降级为成员服务器之一

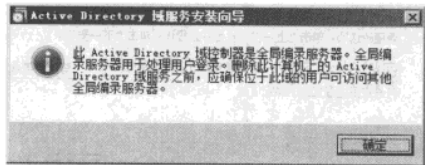


图 7-108 原域控制器降级为成员服务器之二

第 4 步，单击“下一步”按钮，显示如图 7-110 所示的“Administrator 密码”对话框。输入成员服务器上默认管理员账户“Administrator”的密码。

提示 域控制器降级为成员服务器，需要在此输入新管理员的密码。注意，在输入新的管理员密码时，密码必须大、小写字母并且与数字的混合，并且密码必须在 7 位以上。默认管理员账户为“Administrator”。

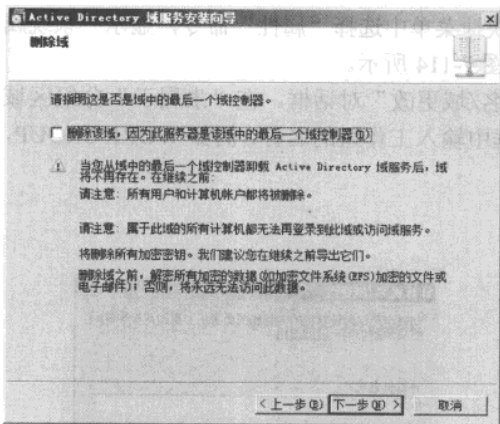


图 7-109 原域控制器降级为成员服务器之三

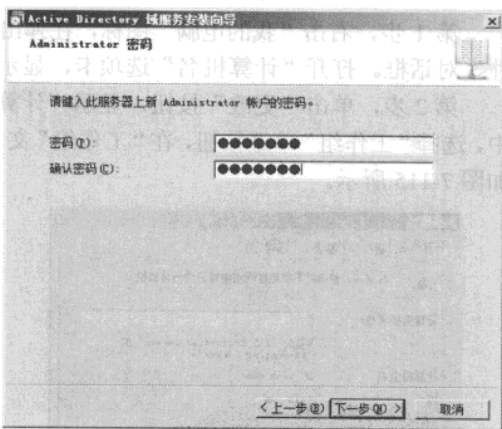


图 7-110 原域控制器降级为成员服务器之四

第 5 步，单击“下一步”按钮，显示如图 7-111 所示的“摘要”对话框。
第 6 步，单击“下一步”按钮，开始删除原域控制器中的 AD DS 域服务，删除完成后显示如图 7-112 所示的“完成 Active Directory 域服务安装向导”对话框。
第 7 步，单击“完成”按钮，显示如图 7-113 所示的“Active Directory 域服务安装向导”对话框。单击“立即重新启动”按钮，重新启动服务器。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

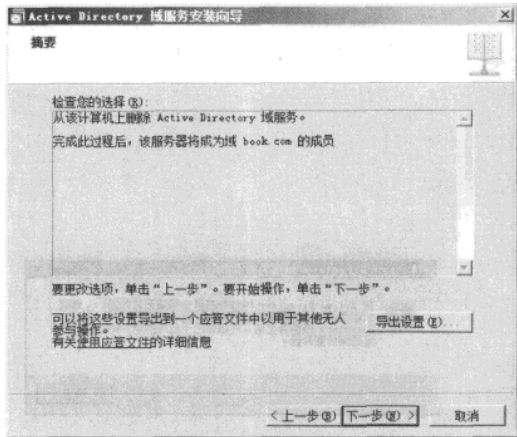


图 7-111 原域控制器降级为成员服务器之五

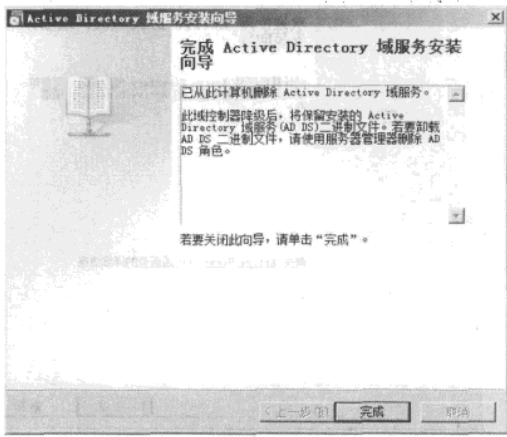


图 7-112 原域控制器降级为成员服务器之六

(6) 成员服务器降级为独立服务器。

成员服务器降级为独立服务器，将成员服务器从域中脱离。重新启动服务器，以本地管理员的身份登录服务器。备份此计算机上的数据至另外的一台计算机或者备份到活动硬盘上，然后用 Windows Server 2008 的安装光盘重新安装 Windows Server 2008，安装过程中 TCP/IP 地址、计算机名等要与原来的一致。

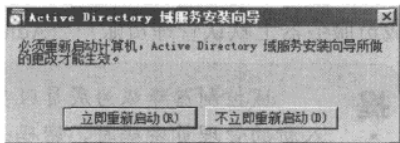


图 7-113 原域控制器降级为成员服务器之七

第 1 步，右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，显示“系统属性”对话框。打开“计算机名”选项卡，显示如图 7-114 所示。

第 2 步，单击“更改”按钮，显示“计算机名/域更改”对话框。在“隶属于”分组区域中，选择“工作组”单选按钮，在“工作组”文本框中输入工作组的名称，例如 WORKGROUP，如图 7-115 所示。

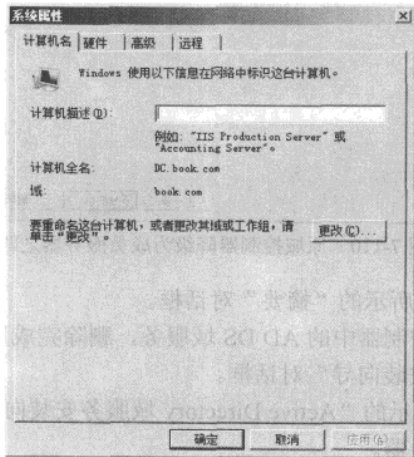


图 7-114 降域之一

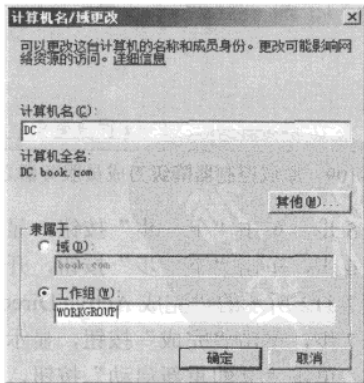


图 7-115 降域之二

第3步，单击“确定”按钮，显示如图 7-116 所示的“Windows 安全”对话框。在“用户名”和“密码”文本框中，输入具备降域用户权限的用户名称和密码。

第4步，单击“确定”按钮，执行降域操作，执行成功后，显示如图 7-117 所示的“计算机名/域更改”对话框。单击“确定”按钮，提示管理员需要重新启动计算机，启动后即可脱离域。

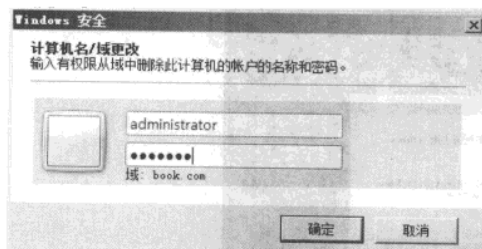


图 7-116 降域之三

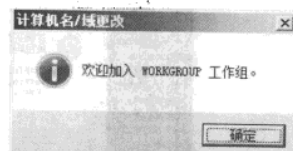


图 7-117 降域之四

第5步，原域控制器故障排除后，重新安装 Windows Server 2008 完成后，先将此计算机升级到额外域控制器，然后再升级到域控制器。

第6步，提升域控制器完成后从备份中恢复数据，至此，Active Directory 域控制器恢复完成。

3. 域控制器彻底损坏且不能恢复

当管理员发现出现此种错误，按照下列步骤将额外域控制器提升为域控制器，重新安装原域控制器，将原域控制器作为额外域控制器使用。

(1) 占用操作主机角色。

当网络中运行 Windows Server 2008 的 Active Directory 域控制器完全损坏并且不能恢复时，需要将网络中的一台额外域控制器“强行”升级为域控制器。

第1步，以域管理员身份登录到额外域控制器，打开命令提示符窗口，启动“ntdsutil”工具，链接到“bdc.book.com”，如图 7-118 所示。

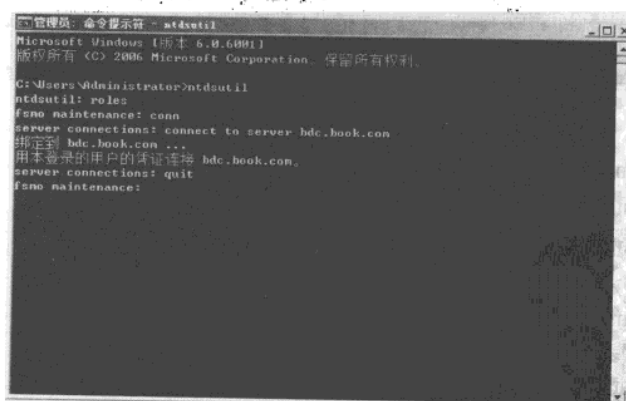


图 7-118 占用“架构主机”角色之一

第2步，占用“架构主机”角色。

① 在 fsmo maintenance 命令提示符下，输入：

网管天下 网管经验谈

Seize schema master

② 按 Enter 键，显示如图 7-119 所示的“角色占用确认对话框”对话框，提示管理员是否需要占用架构主机角色。

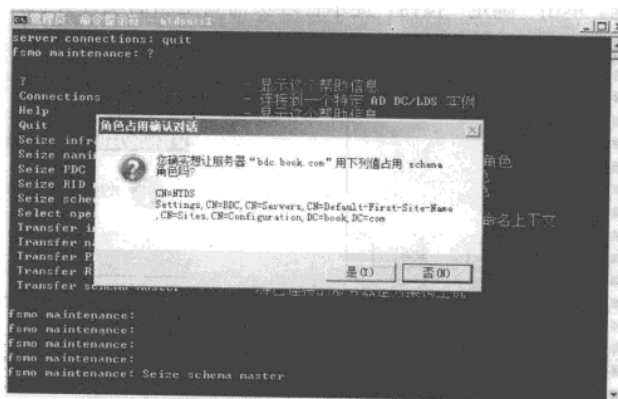


图 7-119 占用“架构主机”角色之二

③ 单击“是”按钮，占用架构主机角色，执行成功后如图 7-120 所示。

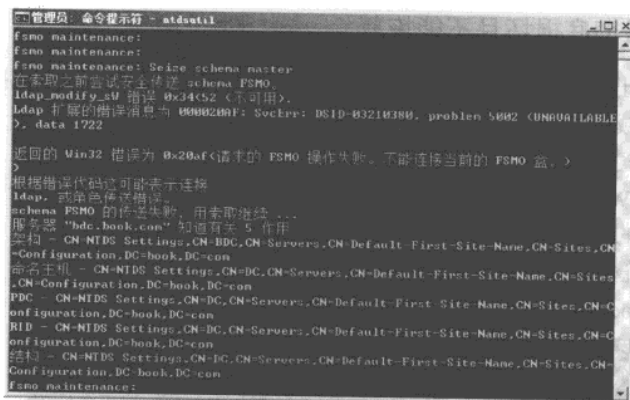


图 7-120 占用“架构主机”角色之三

第 3 步，在 fsmo.maintenance 命令提示符下，分别输入以下命令：

- Seize infrastructure master，占用结构主机角色。
- Seize naming master，占用域命名主机角色。
- Seize PDC，占用 PDC 主机角色。
- Seize RID master，占用 RID 主机角色。

将占用不同操作主机角色。

第 4 步，输入两次“quit”命令，退出 ntdsutil 程序，返回到命令窗口。

(2) 提升额外域控制器为全局编录服务器。

操作过程同“域控制器故障但仍然可用”中的“提升额外域控制器为全局编录服务器”。

第 8 章 网络防病毒系统

随着 Internet 技术的发展，病毒技术也在不断的发展，而且病毒传播途径越来越多，传播速度越来越快，危害越来越大，病毒防御任务更加艰巨，几乎到了令人防不胜防的地步。病毒已经成为计算机使用者的“心腹大患”，尤其在网络中，一旦病毒爆发将严重影响网络的使用，甚至造成网络瘫痪。

8.1 防病毒现状

企业建立网络平台之后，一般都要安装防病毒系统，但是遇到的情况往往都是越想防病毒，反而病毒越来越多，越来越难以清除干净，网络中“中招”的客户端计算机越来越多，管理员只能四处救火，用户抱怨声不断，老板大发脾气。这种病毒防御模式，称之为“被动”防御。根据上述现状可以发现，分散的、各自为政的单一层次的防病毒产品已经难以满足网络防病毒现状的要求，只有建立起覆盖全网的、立体的、集中控制的防病毒体系，并对其实施行之有效的组织管理，才能达到有效防控的目的。

本节将打破这种传统的防病毒系统架构体系，从病毒的传播渠道入手，提倡主动防御的理念，结合传统的被动防御模式，将病毒隔离在网络大门之外，确保网络安全。

8.1.1 病毒传播途径分析

病毒具有自我复制和传播的特点，从病毒的传播机理可知，只要能够进行数据交换的介质都可能成为病毒的传播途径。传统的手工传播病毒的方式与现在通过 Internet 传播相比速度要慢得多。

1. 移动存储设备

可移动设备例如软盘、光盘、磁带、U 盘、移动硬盘、移动电话存储器等，盗版光盘上的软件和游戏，以及非法复制等都是目前传播病毒的主要途径之一。随着大容量可移动存储设备如 Zip 盘、可擦写光盘、磁光盘（MO）、移动硬盘等的普遍使用，这些存储介质也将成为病毒寄生的场所。

硬盘是数据的主要存储介质，因此也是病毒感染的重灾区。硬盘传播病毒的途径主要有：硬盘向软盘上复制带病毒文件，带毒情况下格式化软盘，向光盘上刻录带病毒文件，硬盘之间的数据复制，以及将带病毒文件发送至其他地方等。在移动存储设备中，U 盘是使用最广泛、移动最频繁的存储介质，因此也成了病毒寄生的“温床”。

2. 网络

现代信息技术的巨大进步已使空间距离不再遥远，但也为病毒的传播提供了新的“高速

网管天下 网管经验谈

公路”。病毒可以附着在正常文件中通过网络进入一个又一个系统，而且病毒在计算机网络环境中的传播速度非常快。Internet 已经成为病毒的重灾区，成为木马、恶意软件传播的“温床”。

3. 点对点通信系统和无线网络

目前，这种传播途径还不是十分广泛，但预计在未来的信息时代，这种途径很可能与网络传播途径成为病毒扩散的两大“时尚渠道”。

4. 电子邮件

电子邮件已成为病毒传播的最大载体，与网络之外有邮件往来的邮件服务器，如果没有采取有效的病毒防护措施，极易受到攻击，并会导致病毒在内部网络中快速传播。其实邮件服务器本身不会受到邮件病毒的破坏，只是转发染病毒邮件至用户信箱中，但是当客户机染病毒并产生几何数量级的信件时，邮件服务器会由于在短时间内需转发大量邮件而导致性能迅速下降，直至“宕机”。

8.1.2 网络病毒传播过程分析

单机病毒有时可通过删除带毒文件或低级格式化硬盘等措施将病毒彻底清除，而网络中只要有一台客户端计算机未能清除病毒，就可使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台客户端计算机就有可能被网上另一台带病毒客户端计算机所感染。因此，仅对客户端计算机进行单台病毒清除，并不能有效解决病毒对网络的危害。

在单机环境中，病毒只能通过传输介质从一台计算机到另一台计算机传播，而在网络中则可以通过网络通信机制迅速扩散。典型的 PC 网络在正常使用情况下，只要有一台客户端计算机有病毒，就可在几十分钟内将网内的数百台计算机全部感染。由于病毒在网络中扩散非常快，扩散范围很大，不但能迅速传染局域网内所有计算机，还能通过远程客户端计算机将病毒在短时间内传播到千里之外。因此，网络病毒成为管理员的心腹大患。

1. 网络病毒传播过程

病毒在网络内部之所以能够快速而广泛传播，是因为病毒充分利用了网络的特点。一般来说，计算机网络的基本构成包括服务器和网络结点（包括有盘客户端计算机，无盘客户端计算机和远程客户端计算机）。病毒一般首先通过移动介质、电子邮件或者 Internet 传播给有盘客户端计算机，然后进入网络，进一步在网上传播。具体来说，主要传播方式为：

- 病毒从 Internet、移动设备等感染有盘计算机。如果远程客户端计算机被病毒侵入，病毒通过远程数据交换进入服务器中。
- 病毒直接从有盘计算机复制到服务器中，或者驻留在计算机内存中。
- 客户端计算机访问网络资源时传染给服务器。
- 其他客户端计算机访问服务器时，传染给访问的客户端计算机。

2. 网络病毒危害

从网络病毒在网络上的传播方式可以看出，在网络环境下，网络病毒除了具有可传播性、可执行性、破坏性、可触发性等病毒的共性外，还具有一些新的特点：

- (1) 感染速度快。在单机环境下，病毒只能通过软盘从一台计算机带到另一台计算机，而在网络中则可以通过网络机制迅速扩散。
- (2) 扩散面广。由于病毒在网络中扩散非常快，扩散范围很大，不但能迅速传染局域网内所有计算机，还能在瞬间通过远程客户端计算机将病毒传播到千里之外。
- (3) 传播的形式复杂多样。病毒在网络上一般是通过“客户端计算机—服务器—客户端计算机”的途径进行传播，传播的形式复杂多样。
- (4) 交叉感染，难以彻底清除。单机上的病毒有时可通过删除带病毒文件、低级格式化硬盘等措施将病毒彻底清除。而网络中，只要有一台客户端计算机未能消毒干净，就可能使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台客户端计算机就有可能被网上另一台带病毒客户端计算机所感染。
- (5) 破坏性大。网络上病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络崩溃，破坏数据。

8.1.3 主动防御

主动防御实现的目标，是将病毒尽量阻挡在网关之外。即使病毒渗透进网络，通过 VLAN 的划分，将病毒隔离在小范围之内。

1. VLAN 细化网络

一个 VLAN 相当于一个小的局域网，不同 VLAN 之间默认将不能互相通信。借助 VLAN，可以将物理网络虚拟地划分为若干子网。由于 VLAN 之间的通信必须借助三层设备才能实现，因此可以通过对 IP、MAC 或 VLAN 访问列表的配置，限制 VLAN 之间的通信，进而达到阻隔网络病毒扩散的目的。例如，通过禁止蠕虫病毒使用的敏感端口号，如 135、137、139、445 等 TCP/UDP 端口，即可将蠕虫攻击限制在感染的 VLAN 之内。同时，还可以采用 IP/MAC 地址绑定的方式，防止 ARP 病毒攻击。

2. 网关（防火墙）防御

本方案中的网关指网络出口，一般指连接到 Internet 的出口，通常在网关处部署防火墙。传统的硬件防火墙仅支持对协议层的过滤，阻断未经允许的端口访问。应用层防火墙可以对应用层的数据包进行过滤，拒绝指定的下载格式文件，以及可疑的数据包。

典型的应用层防火墙为 Microsoft ISA Server (ISA)，ISA 不具备杀毒功能但是具备防护病毒入侵的能力，ISA 同时支持防火墙、代理服务器功能。通过 Internet 传播是病毒传播的一大特点，如果禁止用户访问 Internet，即可有效避免被病毒感染的几率。即使允许用户访问 Internet 并开放下载权限，如果禁止“bat”、“exe”、“com”、“cmd”、“pif”等文件类型下载，也可以有效隔离病毒的传播。ISA 通过阻断传输渠道，达到主动防御的目的。

ISA 系统属于应用型系统，需要安装在 Windows Server 服务器中，因此在该服务器中需要部署基于 ISA 的网关防病毒系统，客户端计算机访问的网页或者传输的文件中如果存在病毒，将由网关防病毒系统进行第一次拦截，尽量将通过 Internet 传输的病毒隔离在网关前，此种模式称之为“被动”防御。

网管天下 网管经验谈

3. 计算机隔离

隔离可以理解为网络连接限制。根据管理员定义的策略，隔离服务器可以将客户端计算机的网络连接设置为各种状态。例如，如果一台计算机因缺少关键的安全更新而被视为状态不良，则隔离服务器可以将该计算机置于隔离网络中，使其与网络中其他计算机隔绝，直至恢复健康（安装补丁）为止。如果没有隔离服务器，状态不良的客户端也可以不受限制地访问企业的网络。一旦恶意软件能够通过那些本该由更新程序修补的漏洞危害该计算机，就能够不断试图将自身的感染传播给网络中的其他计算机。

对于已经限制连接并不处理那些状态不良的计算机，隔离服务器提供补救策略，被隔离的计算机无需管理员干预即可纠正影响运行状态的问题。受限的网络允许状态不良的计算机访问安装缺少更新程序必须的特定网络资源，例如 Windows Server Update Services 服务器。客户端计算机被隔离后，状态不良的计算机只能访问那些可使其运行正常的网络资源，在其恢复健康前，不能访问网络中的其他计算机。

4. 更新系统补丁

众所周知，系统漏洞是病毒泛滥的一个主要原因。漏洞发现和修复补丁之间总是存在一定的时间差，而系统漏洞可谓屡见不鲜、层出不穷，其潜在的危险性和危害性也是越来越大。病毒利用系统漏洞大幅泛滥的案例屡见不鲜，最经典的病毒为“冲击波”和“红色代码”。2003 年一场席卷全球的“冲击波”计算机病毒致使成千上万家跨国企业蒙受了惨重的经济损失，而它借助的只是微软操作系统中的一个漏洞，并且在冲击波病毒大肆爆发之前微软已经开发并公布出了弥补漏洞的安全补丁，用户只要及时安装了这些更新就可以安然无恙。

任何一款软件都可能存在漏洞这是不可避免的，更何况是如此庞大的 Windows 操作系统。病毒代码编写人员发现 Windows 漏洞的同时微软的研发人员也会发现，不同的是黑客会用最短的时间编写一个可以借助该漏洞传播的病毒，而微软的 Windows 研发人员则会积极研发弥补这一漏洞的安全补丁，这一过程就是一个同时间赛跑的过程，谁赢得了时间谁就赢得了最后的胜利。但是黑客和微软两方面的实例相差是悬殊的，所以结果也是可想而知的，微软工作人员会在病毒出现之前研发出对应补丁并公布于众，用户只要保证在安全补丁出现后的第一时间安装到自己的计算机上就可以确保自己网络的安全。WSUS 服务器的主要功能就在于此。

5. 部署防火墙

Windows 操作系统中，均内置了防火墙功能，默认情况下，该功能没有启用。管理员可以通过组策略统一启用客户端计算机的防火墙，可以有效的防治其他计算机的非法访问。

8.1.4 被动防御

被动防御，指的是计算机病毒已经参透进网络并感染客户端计算机，利用部署的防病毒系统对病毒进行查杀。或者使用策略，对客户端计算机定期扫描或者清除。

1. 网络防病毒系统

跨区域企业网络，要保证整个广域网安全无毒，首先要保证每一个局域网的安全无毒。

也就是说，一个企业网的防病毒系统是建立在每个局域网的防病毒系统上的。应该根据每个局域网的防病毒要求，建立局域网防病毒控制系统，分别设置有针对性的防病毒策略。从总部到分支机构，由上到下，各个局域网的防病毒系统相结合，最终形成一个立体的、完整的企业网病毒防护体系。

计算机病毒形式及传播途径日趋多样化，网络防病毒工作已不再是简单的单台计算机病毒的检测及清除，需要建立多层次的、立体的病毒防护体系，而且要具备完善的管理系统来设置和维护病毒防护策略。这里的多层次病毒防护体系是指在企业的每台客户端计算机上安装防病毒系统，在服务器上安装基于服务器的防病毒系统，在 Internet 网关上安装基于 Internet 网关的防病毒系统，在邮件服务器中部署邮件防病毒系统。因为对企业来说，防止病毒的攻击并不是保护某一台服务器或客户端计算机，而是从客户端计算机到服务器再到网关以至于每台不同业务应用服务器的全面保护，这样才能保证整个网络不受计算机病毒的侵害。

2. 管理策略

部署网络防病毒系统后，通过集中控管平台，可以对客户端计算机进行强制病毒库更新，或者部署客户端计算机扫描策略，在非工作时间（例如中午），对在线的计算机启用扫描策略，发现病毒后立即清除并以邮件或者其他方式通知管理员，将扫描的结果以日志方式写入到管理服务器中。

8.1.5 网络防病毒体系实现的目标

以“主动”防御为基调，侧重于在病毒进入网络之前部署的防护措施。对于漏网之鱼，部署的网关防病毒系统将进行第一次拦截或者清除，对于进入网络的病毒到达客户端计算机后由部署在客户端计算机中的防病毒系统进行二次拦截或者清除。对于移动设备，在接入计算机时由客户端计算机中的防病毒软件进行扫描和清除，确保病毒不能顺利进入网络。如果病毒没有拦截成功，通过交换机划分的 VLAN，将病毒区域隔离在 VLAN 中，最坏的可能性是感染该 VLAN 中所有客户端计算机，但是不会传染到整个网络中。

“防病毒于网络之外”是终极目标。防病毒系统部署完成后，将管理员从四处救火的状态中解脱出来，将更多的精力用于处理业务系统和学习新知识。

1. 主动防御达到的效果

（1）杜绝病毒体进入网络。

通过对指定类型文件的过滤，将彻底杜绝可疑文件进入网络。病毒离开主体，不能运行也不能传播。

（2）杜绝不安全的计算机进入网络。

通过隔离服务器对没有通过安全策略的客户端计算机进行隔离，强制该类型的客户端计算机在隔离区域进行病毒库升级、安装系统补丁等安全工作，杜绝其直接访问网络资源。

（3）病毒“无计可施”。

网络统一部署安全策略强制及时更新系统补丁，补丁修复成功后，即对某些病毒具备“免疫”能力，即使被感染后，病毒也无计可施。

网管天下 网管经验谈

（4）杜绝病毒泛滥。

VLAN 细化到部门，每个部门中的计算机数量有限，即使在组织单位中爆发病毒，VLAN 也可以有效隔离病毒发作区域，将损失降低到最低程度。

2. 被动防御达到的效果

（1）病毒多层处理。

病毒扫描清理点面结合，采用立体防病毒系统措施，对同一病毒进行多层次处理，将达到更好的防毒效果。

① 在网络的网关处进行网络层病毒包扫描，及时清除蠕虫病毒攻击包，同时对控制病毒传播途径，对未安装防毒软件或未安装补丁的网络结点进行访问控制。对进出网关的邮件进行全面防毒扫描，发现病毒立即处理，并且给出管理员即时通知信息。对进出网关的 Web 访问、FTP 访问行全面防毒扫描，发现病毒立即处理，并且给出管理员即时的通知信息，同时对不良网站和 URL 地址进行过滤，阻挡恶意类型文件。

② 采用数据库比对技术和智能性判断技术，对进出网关的邮件进行垃圾邮件过滤，在网关处将垃圾邮件有效删除掉。

③ 对整个网络内的应用服务器进行全面防护，斩断病毒在服务器内的寄生及传播。

④ 对所有的客户机进行全面防护，彻底消除病毒对客户机的破坏，保证所有客户端计算机都有一个干净、安全的工作平台。

（2）统一升级管理。

所有防病毒系统软件的升级、防毒策略的制定，将通过控管系统集中实现，一方面保证所有防毒软件得到即时更新，另一方面保证整个防毒策略的一致。同时生成整个网络统一的病毒报告日志，便于系统管理人员即时对病毒发现情况进行掌握，制定更加有效的网络平台安全使用策略。

8.2 部署 WSUS 系统更新

安装完成所有 Windows Server 2008 系统补丁后，“Windows Server Update Services（简称 WSUS）”已经作为一个角色添加到“角色添加向导”提供的选择列表中，即 WSUS 作为 Windows Server 2008 的一个组件，而不是一个独立的应用程序。管理员通过添加角色向导即可轻松部署 WSUS 服务器，为网络中的客户端计算机提供系统更新服务。

8.2.1 部署环境

WSUS 在 Windows Server 2008 中作为一个角色，在 Windows Server 2003 作为独立的应用程序，除了支持 Windows 系统（Windows 2000 全系列、Windows XP 全系列和 Windows server 2003 全系列、Windows Vista 全系列、Windows Server 2008 全系列）的更新管理外，还支持 SQL Server、Exchange 2000/2003、Office XP/2003 等系统更新管理。安装 WSUS 角色的计算机称之为 WSUS 服务器。

1. 部署架构

建议采用微软默认的更新服务体系结构，为网络中的客户端计算机以及服务器更新系统补丁，系统架构如图 8-1 所示。部署 WSUS 的服务器硬件要求满足安装 Windows Server 2008 的基本硬件需求即可。

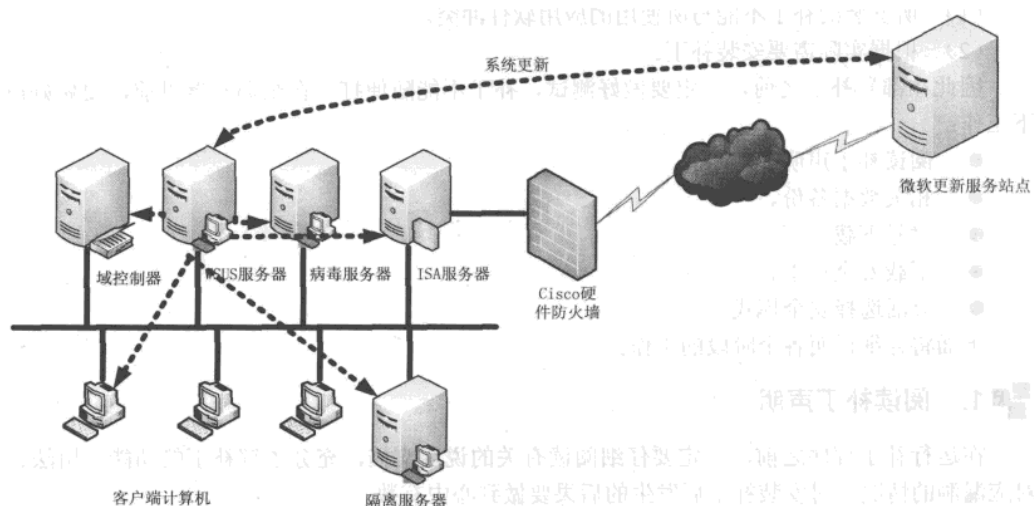


图 8-1 WSUS 部署架构

2. 计算机分组

WSUS 中可以对客户端计算机进行分组，在 WSUS 中内建有两个计算机组：所有计算机和未指定的计算机。默认情况下，任何一个客户端计算机访问 WSUS 服务器时，都将被加入到这两个组中。管理员可以创建计算机组，并将客户端计算机对象从未指定的计算机组中移动到所创建的计算机组中，但是不能将客户端计算机对象从所有计算机组中移动到其他组。这是因为所有计算机组是便于管理员指定将更新程序应用到所有的客户端计算机，而不同的计算机组则便于管理员针对不同的客户端计算机应用不同的更新程序。

3. 后台数据库

WSUS 服务器需要使用数据库存储更新信息，WSUS 数据库存储以下信息：

- WSUS 服务器配置信息。
- 用于描述更新程序作用的元数据。
- 客户端计算机、更新程序信息，以及客户端计算机所进行的更新情况。

管理员不能通过直接访问数据库来管理 WSUS，必须通过 WSUS 管理控制台来进行管理。每个 WSUS 服务器需要自己的数据库，如果具有多个 WSUS 服务器，则必须具有多个 WSUS 数据库。WSUS 支持 Microsoft SQL Server 全系列的数据库产品，建议在部署 WSUS 的服务器中安装 Microsoft SQL Server 2005 SP2 以上版本数据库。如果用户在服务器中没有部署 Microsoft SQL Server 2005 数据库，在安装 WSUS 过程中将自动安装 WSMDE（Windows）桌

面版数据库。

8.2.2 系统补丁部署原则

系统补丁部署的原则：

- (1) 所安装的补丁不能与所使用的应用软件冲突。
- (2) 根据实际需要安装补丁。

因此在部署补丁之前，一定要做好测试，补丁不能随便打。在全局部署以前，要做好以下工作：

- 阅读补丁声明。
- 相关数据备份。
- 对号下载补丁。
- 下载安全补丁。
- 灵活选择安全模式。

下面将详细说明各个阶段的工作。

1. 阅读补丁声明

在运行补丁程序之前，一定要仔细阅读有关的说明文档，充分了解补丁的功能、用法、对应漏洞的情况，对安装补丁后发生的后果要做到心中有数。

然后根据企业的网络环境进行分析，判断可能产生的风险，根据漏洞的紧急情况，判断是否需要安装补丁。

需要提前做好预备工作，确保在补丁安装完成后出现的问题，有高效、快捷、安全的补救措施。

2. 相关数据备份

在安装补丁之前，最好将相关的文件进行备份，以免造成错误，丢失重要数据或者导致系统无法正常运行。

如果是针对操作系统的补丁，确保补丁具备“回滚”功能。

这里的备份包含两部分的内容：

- 原来程序的安装目录。对于绿色软件而言仅需要备份相应的目录即可。
- 系统的 DLL 动态库文件。查明可能覆盖的相关的 DLL 文件，单独备份，确保在安装补丁的时候覆盖了 DLL 文件，如果出现问题，可以将备份的 DLL 文件在操作系统的安全模式下，重新覆盖相关的 DLL 文件。

3. 对号下载补丁

注意补丁程序对应的操作系统和应用软件的版本。很多补丁都是针对某个特定的操作系统和应用软件版本而开发的，如 Windows 2000、Windows XP、Windows Server 2003 和 Windows Vista 所使用的补丁程序即不尽相同，因此，使用的时候要下载与操作系统（还要注意不同语言版本）、应用程序匹配的补丁程序。

4. 下载安全补丁

补丁的来源一定要安全，必须到可靠的平台下载或者到有安全认证的供应商那里获取相关的补丁程序，防止被恶意修改，或者在补丁中安装了“木马”。

一般情况下，建议到官方的网站和信誉较好的网站上下载补丁安装或者在线安装补丁。一方面可以保证下载的补丁是安全有效的，另外可以保证补丁安装包的时效性。

5. 选择安装模式

一般而言，补丁的安装分为在线安装和下载补丁后安装两种模式，可以根据企业的网络状况选择适合自己的安装模式。如果网络环境稳定，可以选择在线安装，否则建议将补丁下载到本地再进行安装，可以有效地避免因为网络原因（线路故障等）造成的安装失败。

在补丁安装的时候，要退出正在运行的应用程序，否则可能会出现因为文件正在使用无法正常安装补丁的情况。

对于系统启动加载的应用程序，尽量将它们从启动项中删除再进行补丁的安装。

总之，在部署补丁的时候，一定要注意补丁的安装策略，否则事与愿违，给工作带来不必要的麻烦。

8.2.3 部署 WSUS 服务器注意事项

安装 Windows 系统补丁程序是完成操作系统安装之后的首要工作，也是确保网络安全和系统正常应用的一道重要屏障。因此，建议用户在每次完成系统安装后，不要立即进行联网或者应用不明的移动存储介质，对于 Windows XP/2003 系统应先启动系统防火墙再进行其他操作。

Windows 系统补丁程序都是由微软网站发布的，用于弥补相应操作系统漏洞或缺陷的应用程序包。通常可以有手动安装和自动安装两种方式。

手动安装补丁程序多用于不支持自动下载和安装更新内容的 Windows 操作系统（如 Windows 98），或者不方便在线获取的更新内容的安装。手动安装补丁程序与普通应用程序的安装比较相似，补丁程序可以通过登录相关网站直接下载，也可以购买含有补丁程序的安装光盘。

在实施系统补丁更新时，应当注意以下问题。

- 计算机在没有安装系统补丁之前切记不要连接到网络，特别是 Internet。所需的补丁程序请使用其他移动存储设备复制到相应的计算机上（Windows XP/2003/ Vista 系统可以启用自带的防火墙后再联网）。
- 注意某些补丁程序对安装顺序的要求，例如 Windows 2000 的某些系统补丁程序就必须要求先安装 SP4 或者 SP1，否则将无法完成安装。
- 开始安装补丁程序前应首先关闭其他应用程序，以免导致安装失败。另外，有些补丁程序安装完成后需要重新启动计算机方可生效，打开的应用程序应注意及时保存。
- 获取补丁程序时应注意其版本要求，不仅要注意 Windows 操作系统的类型，还应注意英文版和简体中文版、繁体中文版的区别。

网管天下 网管经验谈

- 安装过程中如需确认或更改安装目录的，建议保持系统默认设置。

1. 设置 WSUS 管理员

部署 WSUS 角色之前，首先需要将 WSUS 所在的计算机添加到 Active Directory 中，即将 WSUS 服务器提升为域成员服务器。为 WSUS 服务器分配一个用户，分配用户后，需要将该用户添加到 WSUS 服务器的本地管理员组中。本案例中使用用于管理员作为 WSUS 服务器的管理员用户，WSUS 服务器确保能连接到 Internet。

2. 设置补丁暂存目录

在安装过程中出现“选择更新源”对话框（如图 8-2 所示）时，单击“浏览”按钮可以重新指定 WSUS 安装目录，但必须保证目标分区文件系统是 NTFS 格式。如果选择该选项，则 WSUS 服务器将下载所有客户端需要的所有更新安装程序，并保存到本地服务器上。如果取消了该选项，则 WSUS 服务器只负责下载更新程序的列表，并控制客户端可以安装的安全更新。

3. 设置数据库

安装过程中出现“数据库选项”对话框（如图 8-3 所示）时，管理员有 3 个选择来指定 WSUS 服务器所使用的数据库，安装向导默认的是 WSUS 安装过程中自动安装的 WSMDE（Windows）数据库，也可以选择本地计算机上已经安装的数据库。如果在上述准备工作中已经安装了 SQL Server 2005 数据库则可以选择第二个选项并在下拉列表框中指定数据库名称。如果没有安装则可以保持默认选项，但用于安装 WSMDE 数据库的目录所在分区同样必须是 NTFS 格式，并保证最少有 2 GB 的自由空间。

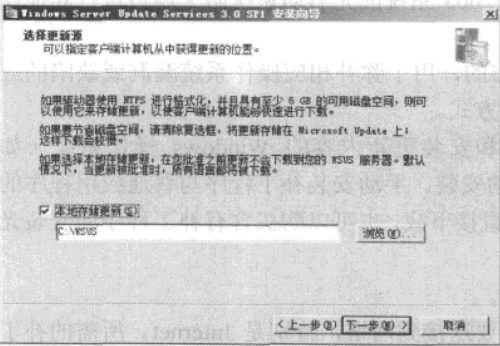


图 8-2 部署 WSUS 角色之十三

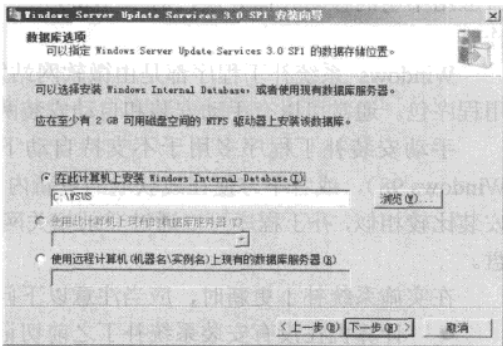


图 8-3 部署 WSUS 角色之十四

4. 设置目标站点

安装过程中出现“网站选择”对话框（如图 8-4 所示）时，选择 WSUS 管理工具和服务网站使用的端口号。选择“使用现有 IIS 默认网站”单选按钮，前提需要在操作系统中安装 IIS 组件。

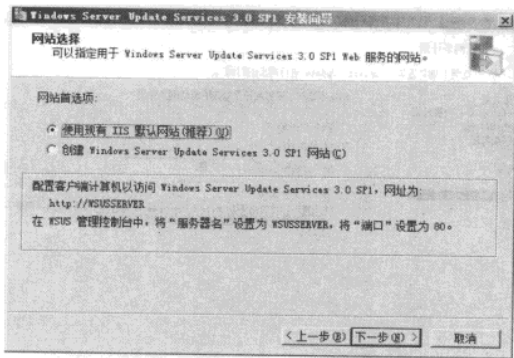


图 8-4 部署 WSUS 角色之十五

5. 设置连接站点

安装过程中出现“选择‘上游服务器’”对话框（如图 8-5 所示）时，将配置 WSUS 服务器连接到的目标站点，如果是中心更新服务器建议连接到微软更新站点，选择“从 Wicrosoft Update 进行同步”单选按钮。该服务器必须能够访问微软的 Update 站点，即可以访问 Internet。

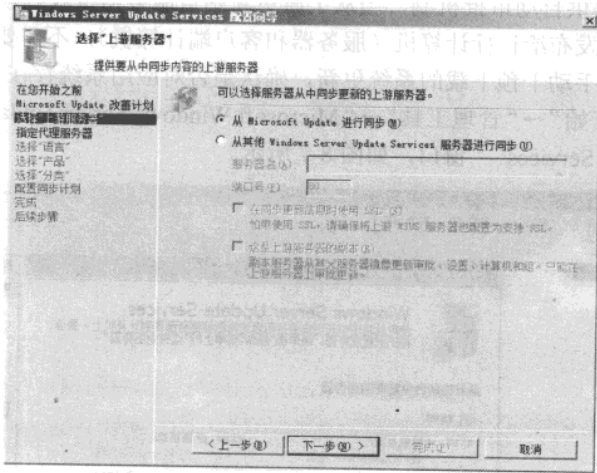


图 8-5 部署 WSUS 角色之二十

6. 设置同步计划

当安装过程中出现“设置同步计划”对话框（如图 8-6 所示）时，设置 WSUS 服务器指定同步计划。如果网络中的客户端数量较多，且类型复杂随时都有获取更新安装程序的需要，则可以给 WSUS 服务器指定一个自动执行的计划，WSUS 自动同步的最高频率为每小时一次。

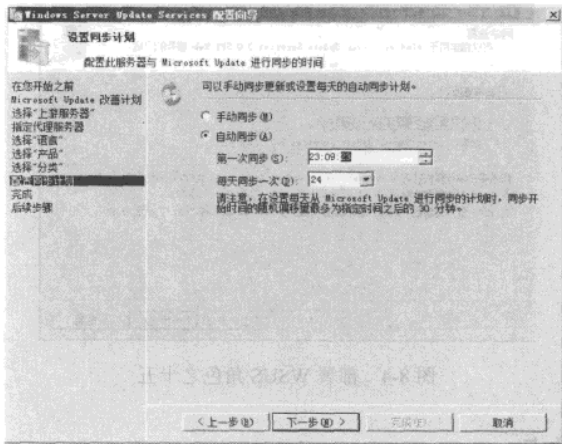


图 8-6 部署 WSUS 角色之二十七

7. 设置自动审批规则

WSUS 服务器提供自动审批机制，当从上游更新站点服务器接收到新的系统更新时，将自动允许接收的更新发布给目标计算机（服务器和客户端计算机），不需要管理员手动干预。在网络中建议管理员手动干预下载的系统更新，确认是否对应用系统存在影响。

第 1 步，选择“开始”→“管理工具”→“Microsoft Windows Server Update Services 3.0 SP1”选项，打开“Update Services”窗口，如图 8-7 所示。



图 8-7 自动审批规则之一

第 2 步，选择“Update Services”→“WSUS（服务器名称）”→“选项”选项，如图 8-8 所示。

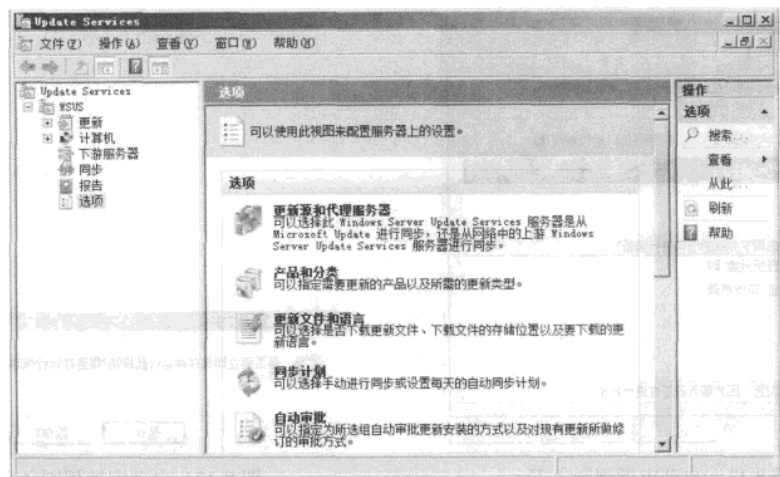


图 8-8 自动审批规则之二

第 3 步，单击“自动审批”超链接，显示如图 8-9 所示的“自动审批”对话框。WSUS 已经默认了一条规则为“默认自动审批规则”，该规则属性为“当更新属于安全更新程序、关键更新程序时，为所有计算机审批更新”。

第 4 步，选择“默认自动审批规则”复选框，单击“安全更新程序、关键更新程序”超链接，显示如图 8-10 所示的“选择‘更新分类’”对话框。如果需要选择所有的系统更新，选择“所有分类”左侧的复选框，否则根据需要选择目标更新。

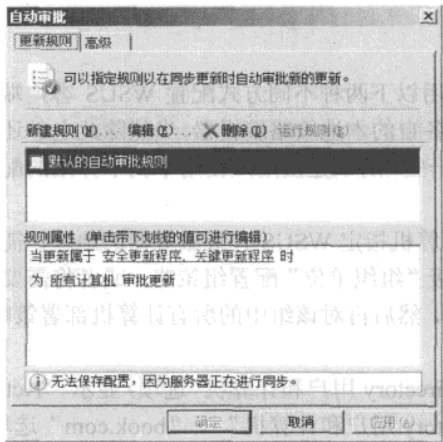


图 8-9 自动审批规则之三

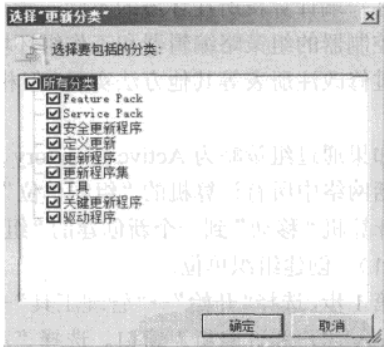


图 8-10 自动审批规则之四

第 5 步，单击“确定”按钮，关闭“选择‘更新分类’”对话框，返回到“自动审批”对话框，如图 8-11 所示规则属性已经更改。

第 6 步，单击“运行规则”按钮，显示如图 8-12 所示的“运行规则”对话框。

第 7 步，单击“是”按钮，运行选择的审批规则。运行完成后，单击“确定”按钮，完成自动审批规则设置。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

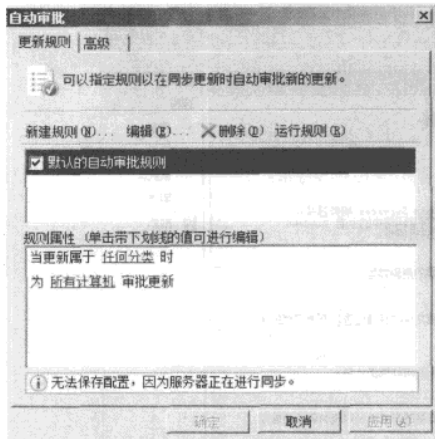


图 8-11 自动审批规则之五

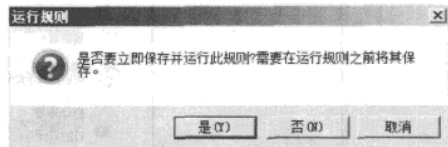


图 8-12 自动审批规则之六

8.2.4 部署客户端计算机系统更新注意事项

WSUS 可以为 Windows 2000 以上操作系统的计算机部署应用更新，在这些系统从 WSUS 获取更新以前，必须进行设置。对于加入到 Active Directory 中的计算机来说，可以通过组策略进行设置。对于没有加入到 Active Directory 的计算机，可以通过运行“gpedit.msc”进行添加设置。

1. 域组策略部署

客户端计算机所在环境的不同，管理员可以采用以下两种不同方式配置 WSUS 客户端，即域控制器的组策略编辑器和工作组环境中客户端各自的本地策略编辑器，当然除此之外还可以通过修改注册表等其他方法实现，但相对要麻烦一些，所以建议用户使用本例中介绍的配置方式。

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器的地址，需要在包括网络中所有计算机的“组织单位”或其上一级“组织单位”配置组策略，或者将需要更新的计算机“移动”到一个新创建的“组织单位”中，然后再对该组中的所有计算机部署策略。

(1) 创建组织单位。

第 1 步，选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，显示“Active Directory 用户和计算机”窗口。选择“Active Directory 用户和计算机”→“book.com”选项，如图 8-13 所示。

第 2 步，右击“book.com”选项，在弹出的快捷菜单中选择“新建”选项，在弹出的级联菜单中选择“组织单位”命令，显示如图 8-14 所示的“新建对象—组织单位”对话框。在“名称”文本框中，输入组织单位的名称。

第 3 步，单击“确定”按钮，完成组织单位的创建。将需要部署系统更新的客户端计算机，移动到新建的组织单位中，移动完成的用户，如图 8-15 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

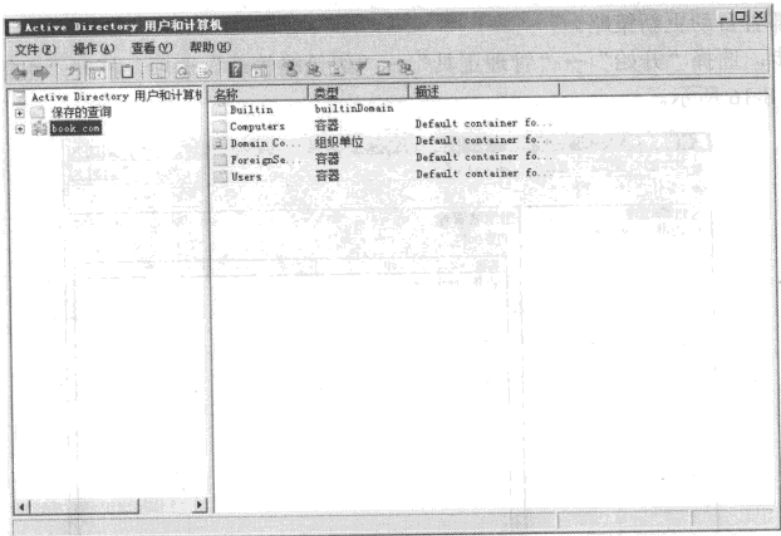


图 8-13 创建组织单位之一

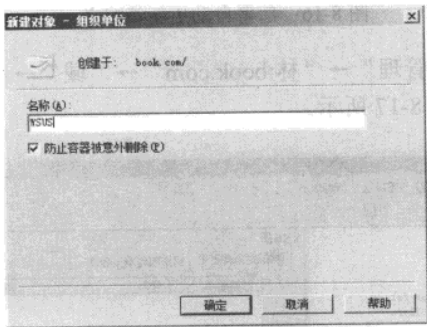


图 8-14 创建组织单位之二

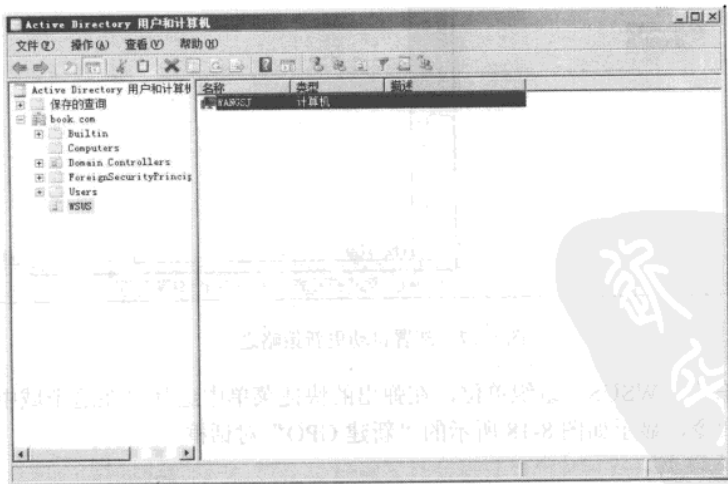


图 8-15 “Active Directory 用户和计算机”控制台

网管天下 网管经验谈

(2) 部署自动更新策略。

第 1 步，选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理”控制台，如图 8-16 所示。

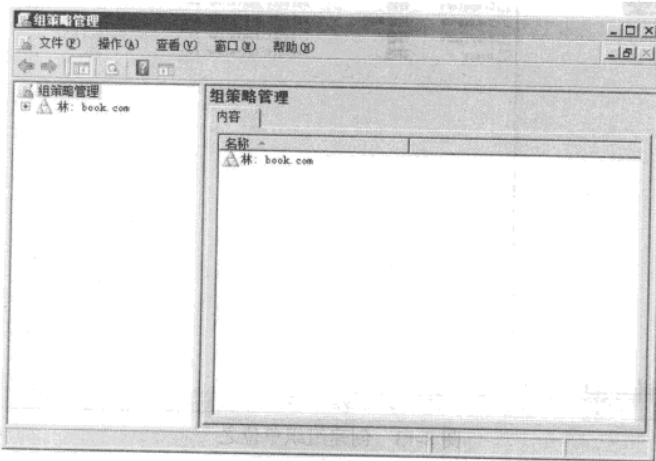


图 8-16 部署自动更新策略之一

第 2 步，选择“组策略管理”→“林:book.com”→“域”→“book.com”，即可查看、创建、修改和删除策略，如图 8-17 所示。

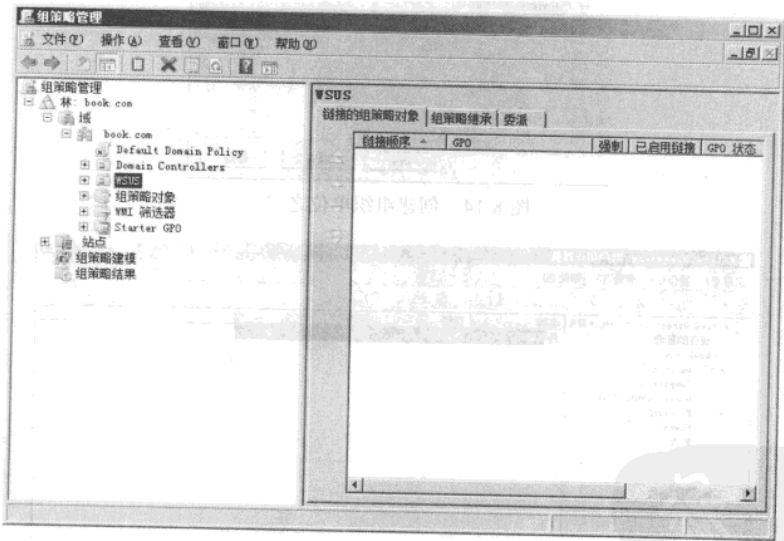


图 8-17 部署自动更新策略之二

第 3 步，右击“WSUS”组织单位，在弹出的快捷菜单中选择“在这个域中创建 GPO 并在此处连接”命令，显示如图 8-18 所示的“新建 GPO”对话框。

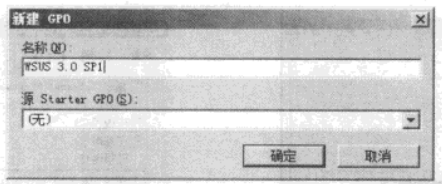


图 8-18 部署自动更新策略之三

第 4 步，单击“确定”按钮，创建新的 GPO 对象。右击新建策略，在弹出的快捷菜单中选择“编辑”命令，打开“组策略管理编辑器”窗口。选择“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“Windows Update”选项，如图 8-19 所示。



图 8-19 部署自动更新策略之四

第 5 步，双击“配置自动更新”策略，显示如图 8-20 所示的“配置自动更新属性”对话框，选择“已启用”单选按钮，激活并选择在“配置自动更新”右侧的下拉列表框中选择对应的自动更新类型，共有 4 种类型，建议选择第 4 种类型“自动下载并计划安装”，即自动下载更新并计划安装，继续设置“计划安装日期”和“计划安装时间”选项，指定执行安装的时间和日期。设置完成后单击“应用”和“确定”按钮保存设置。

第 6 步，双击“指定 Intranet Microsoft 更新服务位置”策略，显示如图 8-21 所示的“指定 Intranet Microsoft 更新服务位置属性”对话框。首先选择“已启用”单选按钮，然后在“设置检测更新的 Intranet 更新服务”文本框中指定局域网中的 WSUS 服务器地址，在“设置 Intranet 统计服务器”文本框中指定用于获取客户端状态信息的服务器地址，本例中使用一台服务器。如果网络中的 WSUS 服务器和统计报表服务器（只用于获取客户端的状态和需求信息）分别是不同的服务器，则此处指定时应特别注意。

网管天下 网管经验谈

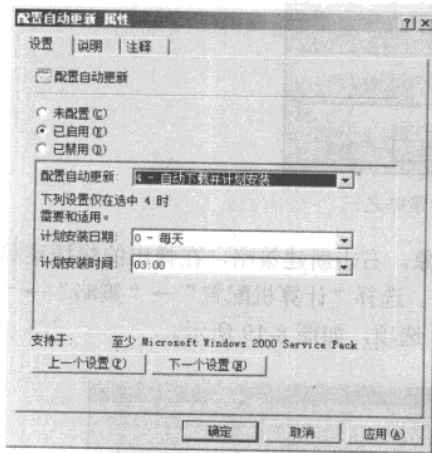


图 8-20 部署自动更新策略之五

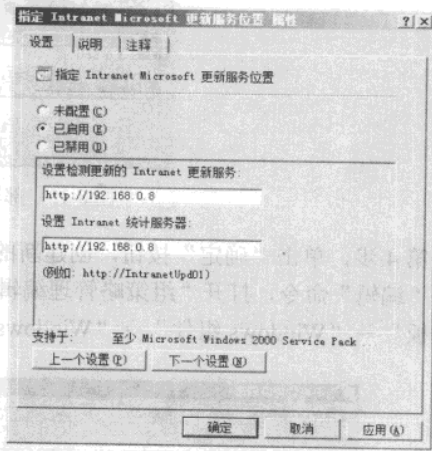


图 8-21 部署自动更新策略之六

第 7 步，单击多次“确定”按钮，保存组策略编辑结果。由于组策略的刷新和应用需要一定的时间，所以保存编辑结果后即使客户端重新登录域控制器了也可能无法立即联系到 WSUS 服务器。而默认情况下，每隔 90 分钟计算机组策略便会在后台刷新一次，刷新的时间可能随机偏移 0~30 分钟，客户端计算机要在域控制器刷新组策略 20 分钟后才可以应用到组策略。如果想要以更快的速度刷新组策略，可以在服务器端设置组策略后，通过运行 gpupdate 命令让设置即时生效，并在客户端计算机通过运行 gpupdate /force 命令立刻生效。如果计算机不是 Active Directory 的成员，可以通过输入 wuauclt.exe /detectnow 来消除 20 分钟延时。

2. 独立计算机策略配置

如果计算机没有加入到 Active Directory，或者想覆盖 Active Directory 中通过组策略指定的 WSUS 升级服务器的地址或配置，可以在客户端计算机上通过运行“Gpedit.msc”，并从“计算机配置”→“管理模板”→“Windows 组件”→“Windows Update”中进行设置。

第 1 步，选择“开始”→“运行”选项，打开如图 8-22 所示的“运行”对话框，输入“gpedit.msc”命令。

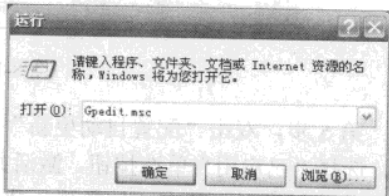


图 8-22 本地策略配置客户端计算机之一

第 2 步，单击“确定”按钮，打开组策略编辑器，选择“计算机配置”→“管理模板”→“Windows 组件”→“Windows Update”选项，双击右侧的“配置自动更新”选项，在“配置自动更新属性”对话框（如图 8-23 所示）中启用自动更新并选择自动更新的方式。如果选择了“自动下载并通知安装”选项，则需要设置“计划安装日期”和“计划安装时间”。

第 3 步，单击“下一设置”按钮，显示“指定 Internet Microsoft 更新服务位置属性”对话框（如图 8-24 所示）。启用内部更新并指定升级服务器的地址，格式为 http://WSUS 服务器 IP 地址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

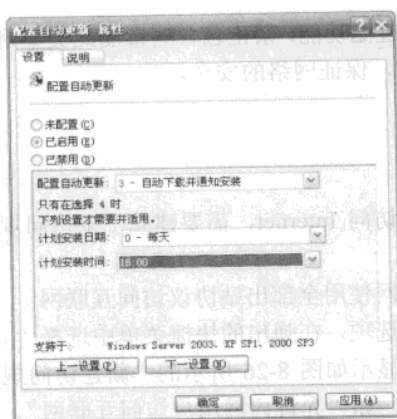


图 8-23 本地策略配置客户端计算机之二

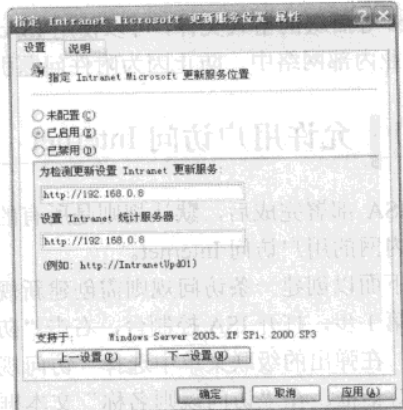


图 8-24 本地策略配置客户端计算机之三

第 4 步，最后单击“确定”按钮，保存所有设置即可。需要注意，保存本地策略修改后并不会立即生效，也需要一定的等待时间。当然也可以使用强制刷新本地策略的方法使其立即生效，即在命令提示符窗口中运行 `gpupdate /force` 命令行，显示如图 8-25 所示的结果即表明刷新成功。生效之后，客户机会自动联系 WSUS 服务器进行升级。



图 8-25 本地策略配置客户端计算机之四

8.3 部署应用层防火墙

网络中部署防病毒系统，属于“被动”防御。管理员可以通过防火墙部署“主动”防御策略，将病毒阻挡在网络之外。本节以 ISA 为例说明如何部署“主动”防御策略，以及 ISA 部署过程。

ISA 是一款性能优异的防火墙产品，可以提高网络的安全性和运行性能，需要注意的是，它不具有杀毒功能。网络管理员可以创建防火墙策略，禁止可执行文件的下载，例如 exe、com、bat、pif、scr 和 vbs 等后缀的格式文件，同时可以禁止浏览器插件的下载，例如 dll 和 ocx 等，保证病毒程序主体文件不能通过网络下载的方式进入企业内部网络中，像一层虚拟的病毒防火墙阻挡病毒的进入，对病毒来说，等于关上了大门。邮件附件中的 exe、com、bat、pif、scr

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

和 vbs 等后缀的格式文件，可以使用 ISA 的邮件附件过滤功能，禁止包含病毒的此类型附件进入企业内部网络中，防止因为附件问题引起病毒泛滥，保证网络的安全。

8.3.1 允许用户访问 Internet

ISA 部署完成后，默认规则是所有的用户都不能访问 Internet，需要建立一条访问规则，允许内网的用户访问 Internet。

下面以创建一条访问规则需创建新规则，允许内网使用全部出站协议访问互联网。

第 1 步，打开 ISA 控制台，右击“防火墙策略”选项，在弹出的快捷菜单中选择“新建”命令，在弹出的级联菜单中选择“访问规则”命令，显示如图 8-26 所示的“新建访问规则向导”对话框。在“访问规则名称”文本框中设置规则，如“允许内网用户访问互联网”。

第 2 步，单击“下一步”按钮，显示如图 8-27 所示的“规则操作”对话框。在对话框中，选择“允许”单选按钮。

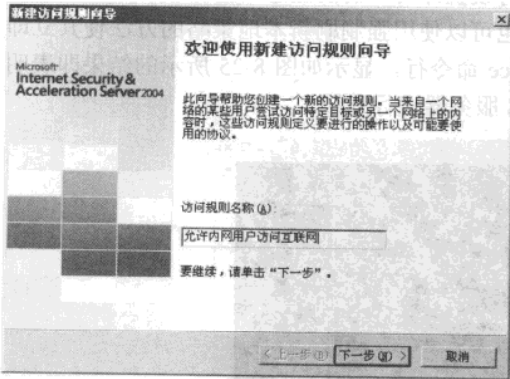


图 8-26 允许内网用户访问互联网之一

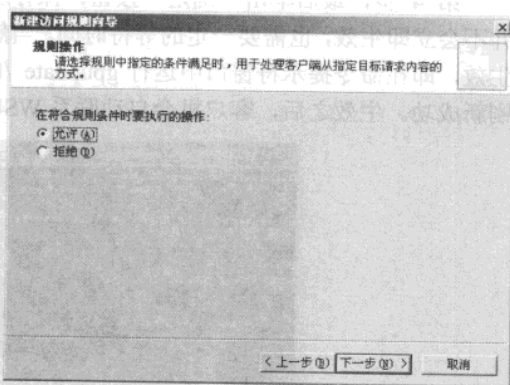


图 8-27 允许内网用户访问互联网之二

第 3 步，单击“下一步”按钮，显示如图 8-28 所示的“协议”对话框。在“协议”对话框中，选择“此规则应用到”下拉列表框中的“所有出站通信”选项。

第 4 步，单击“下一步”按钮，显示如图 8-29 所示的“访问规则源”对话框。

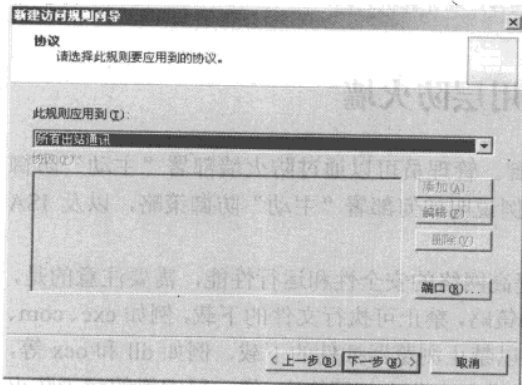


图 8-28 允许内网用户访问互联网之三

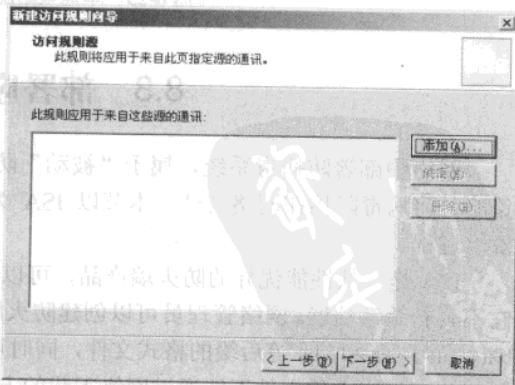


图 8-29 允许内网用户访问互联网之四

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 5 步，单击“添加”按钮，显示如图 8-30 所示的“添加网络实体”对话框，选择“内部”选项。

第 6 步，单击“添加”按钮，完成访问规则源的添加，设置完成的访问规则源如图 8-31 所示。

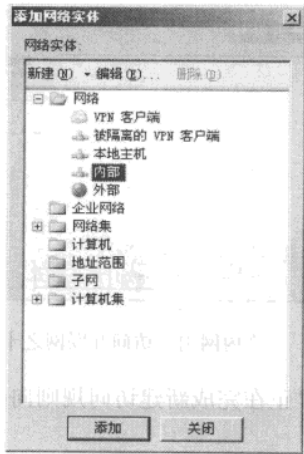


图 8-30 允许内网用户访问互联网之五

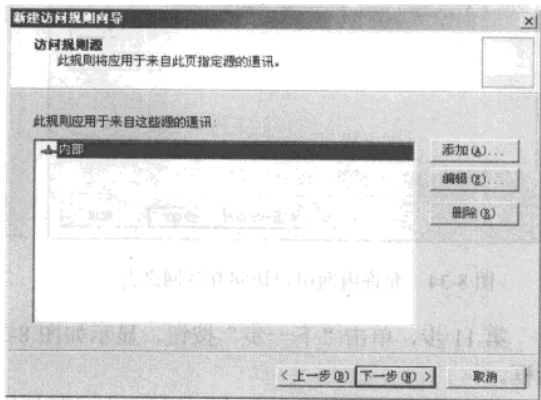


图 8-31 允许内网用户访问互联网之六

第 7 步，单击“下一步”按钮，显示如图 8-32 所示的“访问规则目标”对话框。

第 8 步，单击“添加”按钮，显示如图 8-33 所示的“添加网络实体”对话框。在“添加网络实体”对话框中，选择“外部”选项。

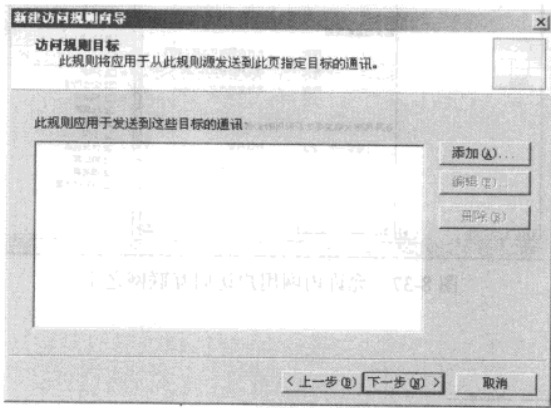


图 8-32 允许内网用户访问互联网之七

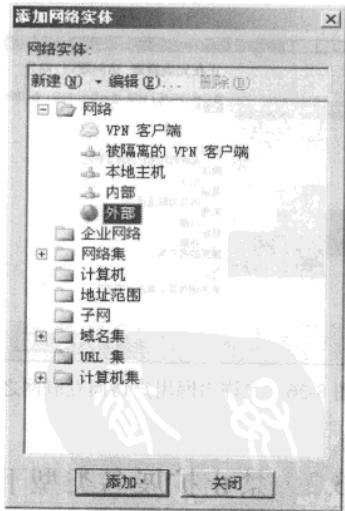


图 8-33 允许内网用户访问互联网之八

第 9 步，单击“添加”按钮，完成访问规则目标的添加，设置完成的访问规则目标如图 8-34 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 10 步，单击“下一步”按钮，显示如图 8-35 所示的“用户集”对话框，默认选择“所有用户”。

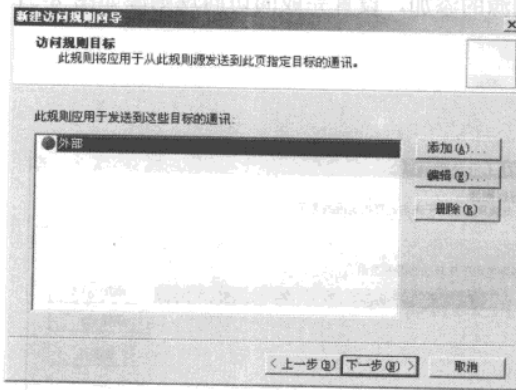


图 8-34 允许内网用户访问互联网之九

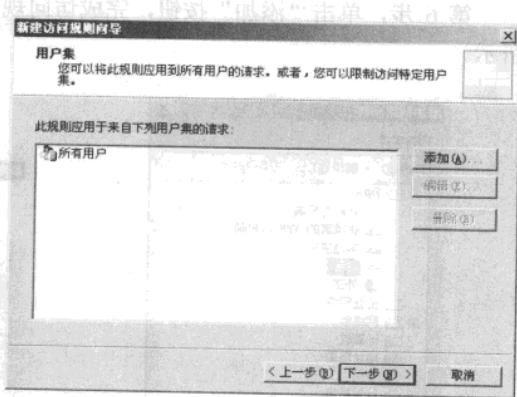


图 8-35 允许内网用户访问互联网之十

第 11 步，单击“下一步”按钮，显示如图 8-36 所示的“正在完成新建访问规则向导”对话框。

第 12 步，最后单击“完成”按钮，完成新规则的创建。当新规则创建完成以后，单击“应用”按钮使规则生效，内网用户就可以访问外部 Web 站点了，如图 8-37 所示。

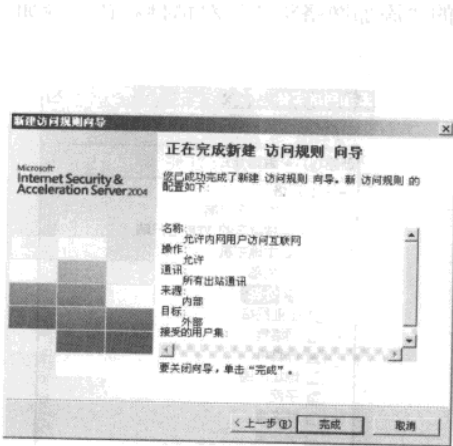


图 8-36 允许内网用户访问互联网之十一

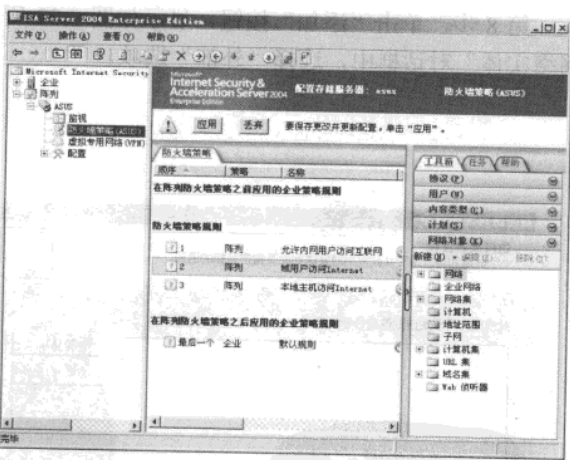


图 8-37 允许内网用户访问互联网之十二

8.3.2 禁止扩展名类型下载

允许员工访问 Internet，但是不允许下载或者访问带有恶性性质的软件。网页病毒、木马都是通过用户访问 Internet 时入侵网络的，一般的病毒文件格式为 exe、com、vbs、bat、scr、pif、dll、ocx 等，一旦进入网络中将影响网络的整体安全。在 ISA 中，使用 HTTP 过滤器，可

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以对文件的扩展名进行阻止。例如，过滤当前网页中含有“.exe”等可执行文件。

第 1 步，在 ISA 控制台的“防火墙策略”窗口中，右击已创建的规则“允许内网用户访问互联网”策略，在弹出的快捷菜单中选择“配置 HTTP”命令，打开“为规则配置 HTTP 策略”对话框，如图 8-38 所示。

第 2 步，打开“扩展名”选项卡，在“指定对文件扩展名要执行的操作”下拉列表框中选择“阻止指定的扩展名（允许所有其他扩展名）”选项，如图 8-39 所示。

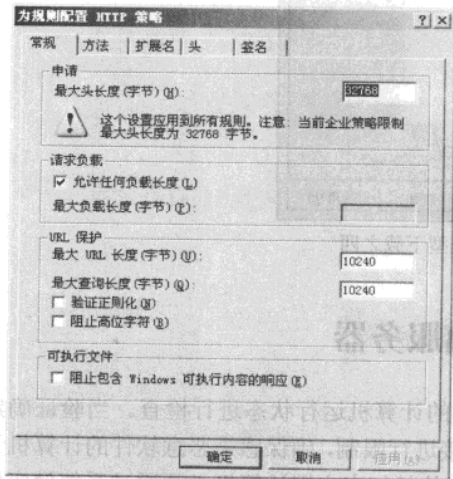


图 8-38 禁止扩展名类型下载之一

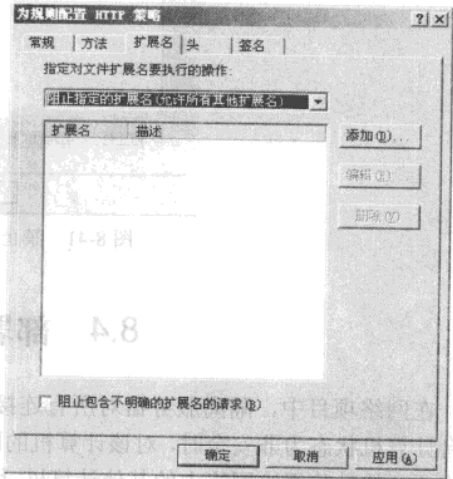


图 8-39 禁止扩展名类型下载之二

第 3 步，单击“添加”按钮，显示“扩展名”对话框，在“扩展名”文本框中输入文件扩展名，如“.exe”，在“描述”文本框中输入说明信息，如图 8-40 所示。单击“确定”按钮，添加到“扩展名”选项卡。

第 4 步，按照同样步骤，添加其他扩展，如“.torrent”等，并且在“扩展名”选项卡中选择“阻止包含不明确的扩展名的请求”复选框，如图 8-41 所示。

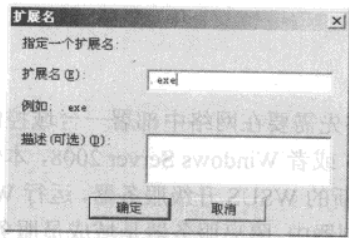


图 8-40 禁止扩展名类型下载之三

第 5 步，设置完成后，单击“确定”按钮即可。

第 6 步，当规则修改完成以后，单击“应用”按钮使规则生效。

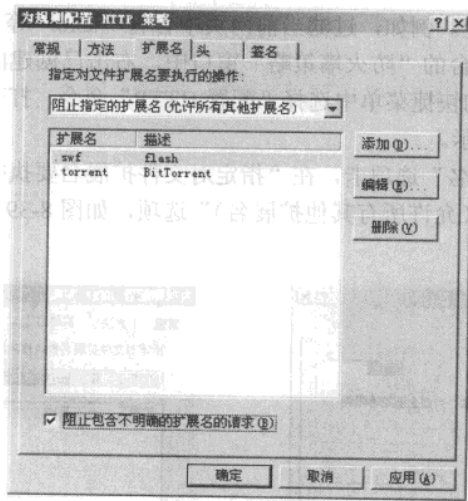


图 8-41 禁止扩展名类型下载之四

8.4 部署隔离服务器

在网络项目中，隔离服务器对所有连接到网络的计算机运行状态进行检查。当验证确定一台计算机状态为非安全时，对该计算机的网络连接进行限制，确保感染恶意软件的计算机无法将恶意软件传播给网络中的其他计算机。用户隔离使任何客户端计算机必须通过系统健康检查（安装最新的安全补丁、防病毒软件的特征库更新、启用防火墙、启用自动更新功能等）且符合安全条件后才允许连接网络。未通过系统健康检查的计算机将被隔离到一个受限制网络，在受限制访问网络中，修复计算机的状态并达到网络健康标准（从补丁服务器下载补丁，强制开启防火墙等）后，才允许接入网络。本章以 DHCP 用户强制隔离为例，说明如何在网络中部署用户隔离功能。

8.4.1 部署隔离服务器

1. 隔离架构

在部署隔离服务器之前，首先需要在网络中部署一台域控制器，该域控制器运行的操作系统可以是 Windows Server 2003 或者 Windows Server 2008，本例中运行 Windows Server 2008 操作系统。部署一台用于补丁更新的 WSUS 升级服务器，运行 Windows Server 2008 操作系统。本例中，DHCP 服务部署在域控制器中，隔离服务器是域成员服务器，运行 Windows Server 2008 操作系统，以域管理员身份登录，系统架构如图 8-42 所示。隔离服务器硬件要求满足安装 Windows Server 2008 的基本硬件需求即可。

用户隔离服务器，完成策略部署。包括以下内容：

- 配置新的 DHCP 作用域。网络中的客户端计算机正常分配网络参数，受限计算机得到非正常的 DNS 地址其他参数正常，受限计算机将不能连接到域中。

- 配置隔离策略。启用 DHCP 强制隔离策略，不满足该条件的计算机将视为受限计算机。
- 网络内部署隔离策略。通过组策略部署系列策略，完成网络内登录计算机的验证。

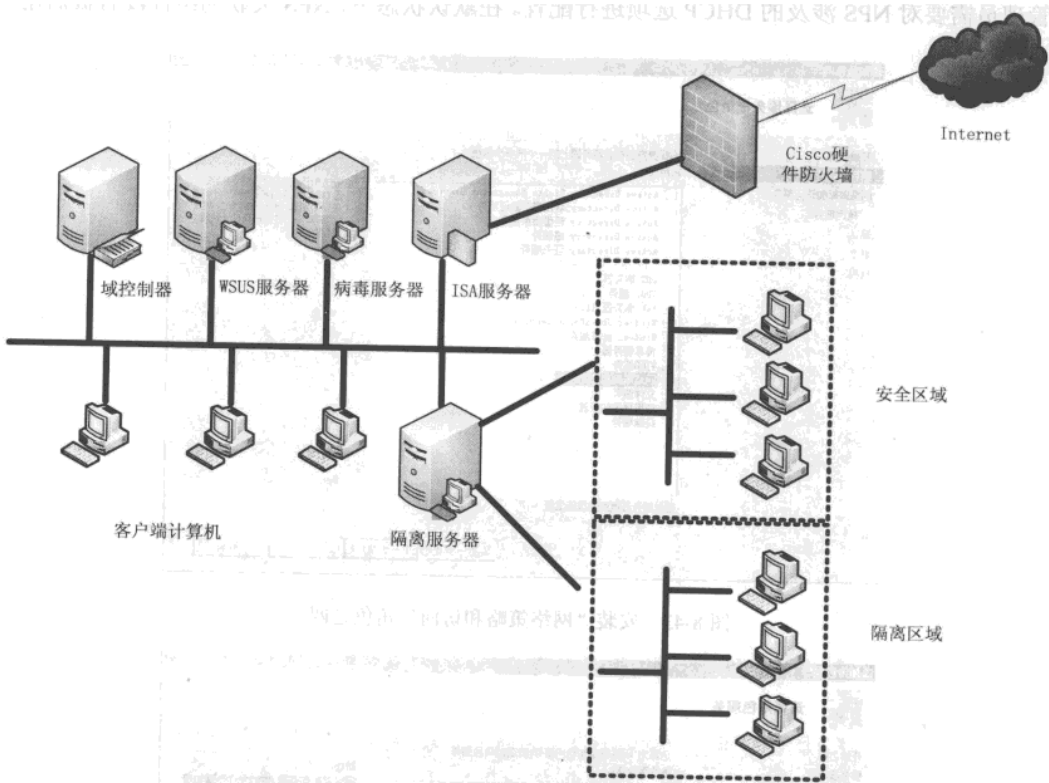


图 8-42 隔离架构

2. 域控制器安装“DHCP 服务器”角色

Windows Server 2008 安装完成后，默认没有安装 DHCP，需要网络管理员在服务器管理器中添加 DHCP 服务器角色。在安装过程中，设置目标作用域并选择激活 DHCP 服务器选项。

3. 安装“网络策略和访问”角色

隔离服务器，加入域并以域管理员身份登录，在该服务器中部署“网络策略和访问”角色。在“服务器管理器”窗口中，通过“添加角色”向导安装该角色即可。

在安装过程中出现“选择服务器角色”对话框时，在“角色”列表框中，选择“网络策略和访问服务”选项，如图 8-43 所示。

当出现“选择角色服务”对话框时，在“角色服务”列表框中，选择“网络策略服务器”复选框，然后根据向导默认安装即可，如图 8-44 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4. 配置 DHCP 作用域

安装完成 NPS 服务后，成员服务器中的 DHCP 服务将被新的包含 NPS 功能的组件更新，管理员需要对 NPS 涉及的 DHCP 选项进行配置。在默认状态下，NPS 关联的组件没有被启用。

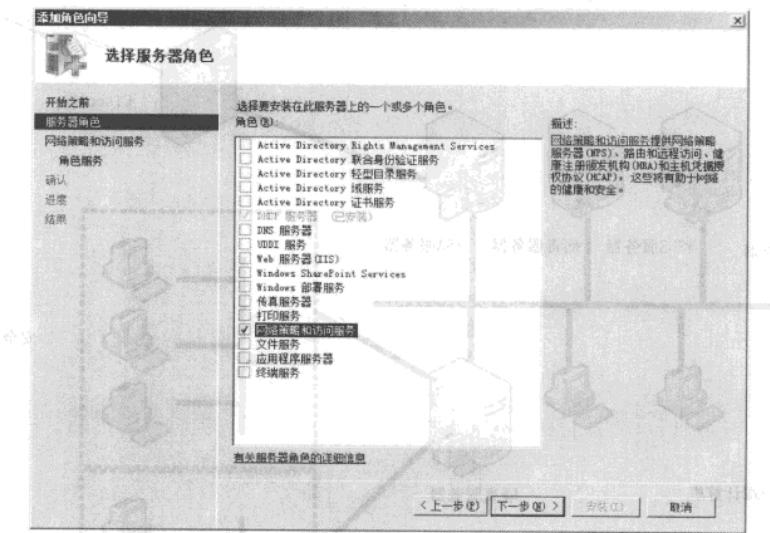


图 8-43 安装“网络策略和访问”角色之四

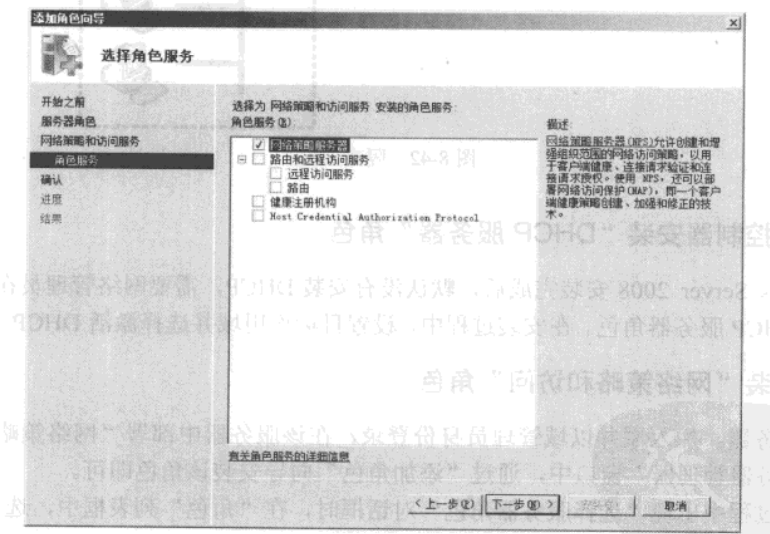


图 8-44 安装“网络策略和访问”角色之六

(1) 配置 DHCP 作用域。

Windows Server 2008 的 DHCP 服务和以前版本不同，DHCP 部署和 NPS 安装完成后，在 DHCP 作用域属性中添加“网络访问保护”选项卡，默认情况下，该设置没有启用，需要管

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

理员启用该设置。

第 1 步，选择“开始”→“管理工具”→“DHCP”选项，显示如图 8-45 所示的“DHCP”管理控制台窗口。

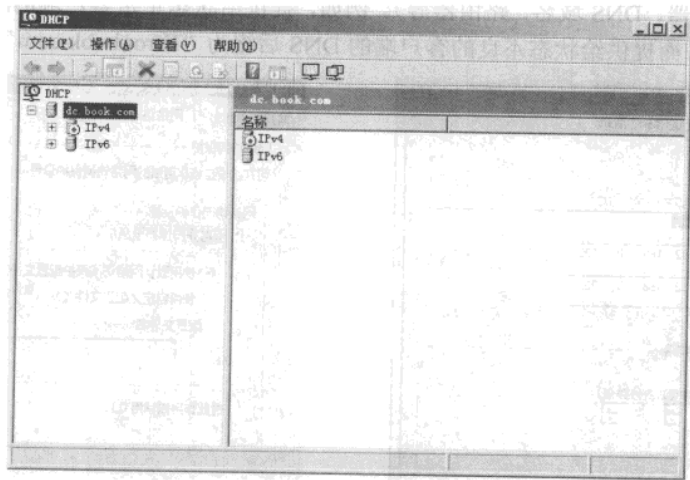


图 8-45 配置 DHCP 作用域之一

第 2 步，选择“DHCP”→“dc.book.com”→“IPv 4”→“作用域[192.168.0.0]”选项，如图 8-46 所示。

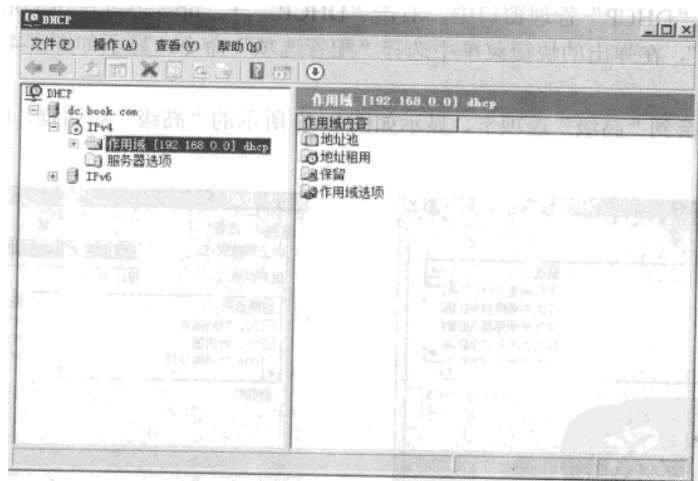


图 8-46 配置 DHCP 作用域之二

第 3 步，右击“作用域[192.168.0.0]”选项，在弹出的快捷菜单中选择“属性”命令，显示如图 8-47 所示的“作用域[192.168.0.0]dhcp 属性”对话框。

第 4 步，切换到“网络访问保护”选项卡，选择“网络访问保护设置”分组区域中的“对此作用域启用”单选按钮，启用网络访问保护功能，如图 8-48 所示。

第 5 步，单击“确定”按钮，配置完成作用域的网络服务保护属性。

网管天下 网管经验谈

(2) 配置 DHCP 服务器选项。

隔离服务器通过 DHCP “用户类作用域” 选项，使计算机在同一作用域内的受限网络和不受限网络访问之间切换。在向状态不良的客户端计算机提供租约时，会使用这组特殊的作用域选项（DNS 服务器、DNS 域名、路由器等）。例如，提供给状态正常客户端的默认 DNS 后缀为 “book.com”，而提供给状态不良的客户端的 DNS 后缀为 “Error.book.com”。

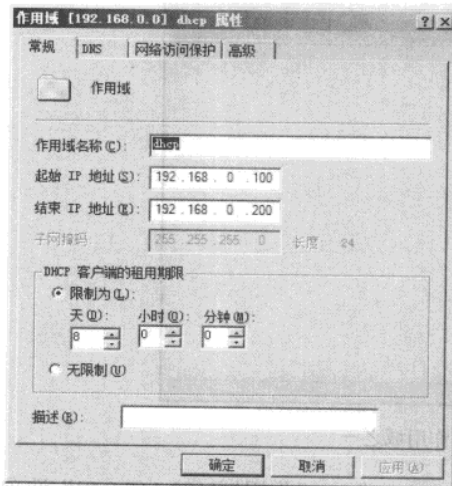


图 8-47 配置 DHCP 作用域之三

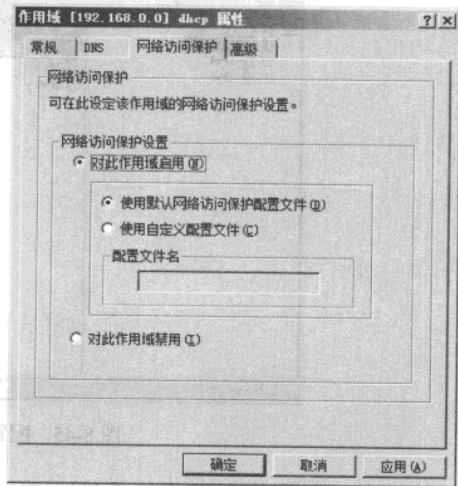


图 8-48 配置 DHCP 作用域之四

第 1 步，在 “DHCP” 管理窗口中，右击 “DHCP” → “npsserver.book.com” → “IPv 4” → “服务器选项”，在弹出的快捷菜单中选择 “配置选项” 命令，显示如图 8-49 所示的 “服务器选项” 对话框。

第 2 步，切换到 “高级” 选项卡，显示如图 8-50 所示的 “高级” 对话框，配置正常 DHCP 服务器选项。

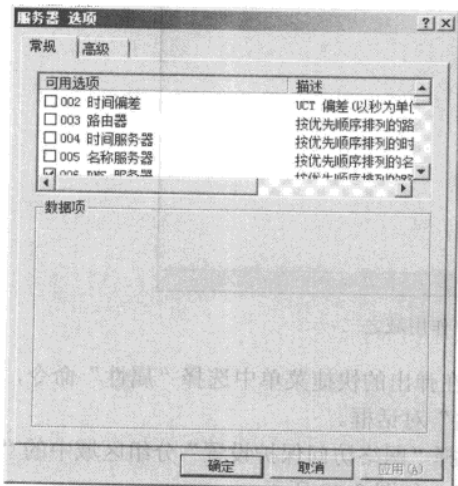


图 8-49 配置服务器选项之一

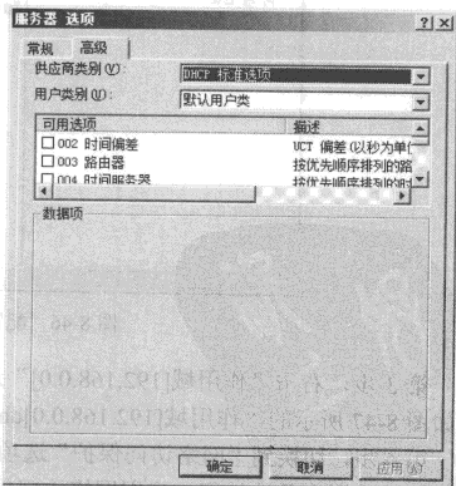


图 8-50 配置服务器选项之二

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- ① 在“供应商类别”下拉列表框中，选择“DHCP 标准选项”选项。
- ② 在“用户类别”下拉列表框中，选择“默认用户类”选项。
- ③ 在“可用选项”列表框中，选择“003 路由器”复选框，在“IP 地址”文本框中输入网络中路由器使用的 IP 地址，例如 192.168.0.1，单击“添加”按钮。如果网络中有多个路由器，可以再次添加。如果发现路由器的顺序错误，可以单击“向下”或者“向上”按钮调整路由器的顺序，如图 8-51 所示。
- ④ 在“可用选项”列表框中，选择“006 DNS 服务器”复选框，在“IP 地址”文本框中输入网络中 DNS 服务器使用的 IP 地址，例如 192.168.0.1，单击“添加”按钮。如果网络中有多个 DNS，可以再次添加。如果发现 DNS 服务器的顺序错误，可以单击“向下”或者“向上”按钮调整 DNS 服务器的顺序，如图 8-52 所示。

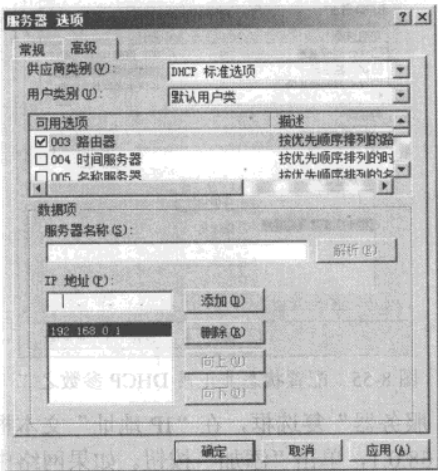


图 8-51 配置状态正常 DHCP 参数之一

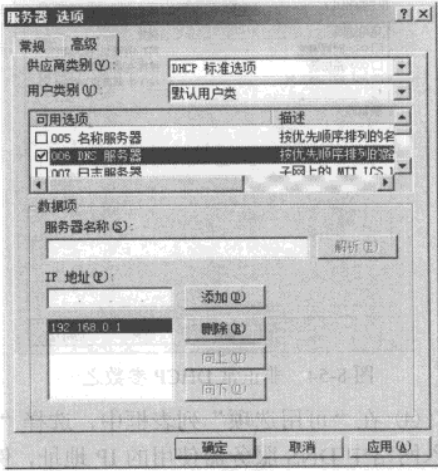


图 8-52 配置状态正常 DHCP 参数之二

- ⑤ 在“可用选项”列表框中，选择“015 DNS 域名”复选框，在“数据项”分组区域的“字符串值”文本框中输入正常解析的 DNS 域名，即 book.com，如图 8-53 所示。

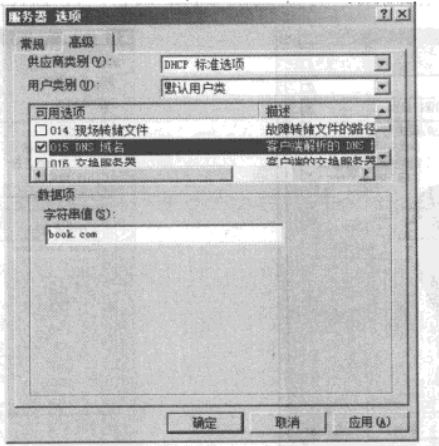


图 8-53 配置状态正常 DHCP 参数之三

网管天下 网管经验谈

第 3 步，配置隔离保护的服务器选项，该选项适用于没有通过 NAP 客户端代理认证的计算机，由 DHCP 分配的网络参数。

- ① 在“供应商类别”下拉列表框中，选择“DHCP 标准选项”选项。
- ② 在“用户类别”下拉列表框中，选择“默认的网络访问保护级别”选项，如图 8-54 所示。
- ③ 在“可用选项”列表框中，选择“003 路由器”复选框，在“IP 地址”文本框中输入网络中路由器使用的 IP 地址，例如 192.168.0.1，单击“添加”按钮。如果网络中有多个路由器，可以再次添加。如果发现路由器的顺序错误，可以单击“向下”或者“向上”按钮调整路由器的顺序，如图 8-55 所示。

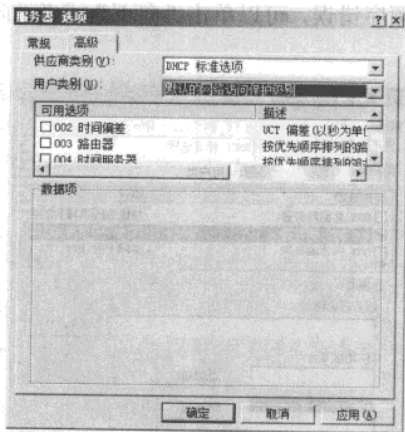


图 8-54 非正常 DHCP 参数之一

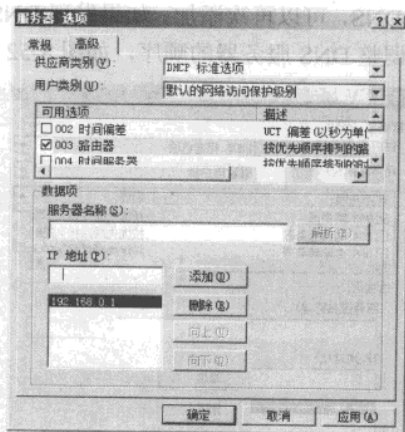


图 8-55 配置状态非正常 DHCP 参数之二

- ④ 在“可用选项”列表框中，选择“006 DNS 服务器”复选框，在“IP 地址”文本框中输入网络中 DNS 服务器使用的 IP 地址，例如 192.168.0.1，单击“添加”按钮。如果网络中有多个 DNS，可以再次添加。如果发现 DNS 服务器的顺序错误，可以单击“向下”或者“向上”按钮调整 DNS 服务器的顺序，如图 8-56 所示。
- ⑤ 在“可用选项”列表框中，选择“015 DNS 域名”复选框，在“数据项”分组区域的“字符串值”文本框中输入隔离用户分配到的 DNS 域名，即 Error.book.com，如图 8-57 所示。

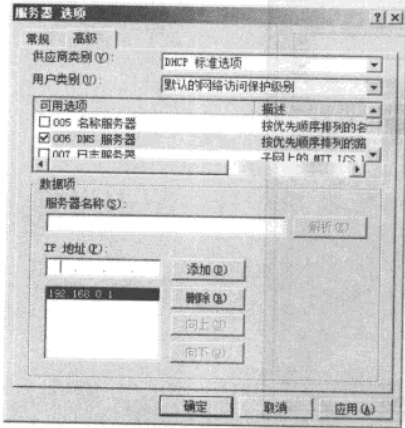


图 8-56 配置状态非正常 DHCP 参数之三

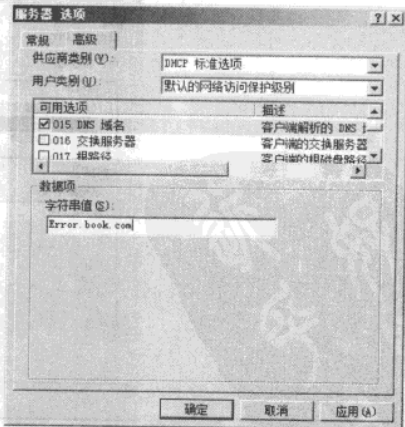


图 8-57 配置状态非正常 DHCP 参数之四

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示 此域名和 DHCP 安装过程创建的域名不同，没有实际的作用，只是方便管理员区分连到网络中的计算机哪些是安全的，哪些是不安全的。例如，如果计算机是安全的，将使用 Book.com 域名，如果计算机不是安全的，将使用

第 4 步，单击“确定”按钮，完成服务器选项的设置，如图 8-58 所示。

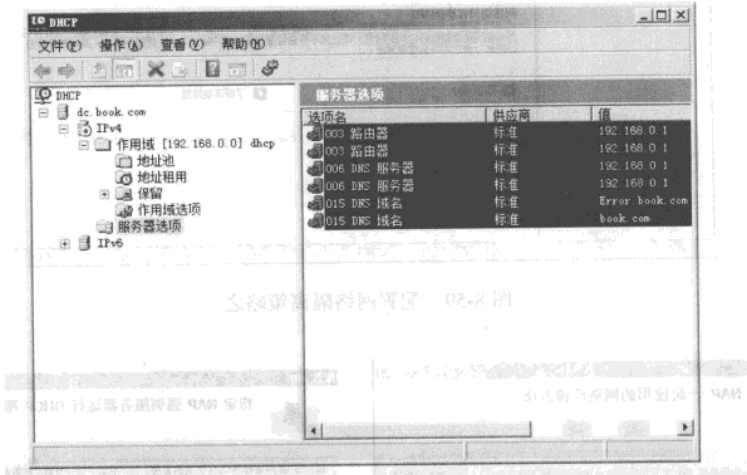


图 8-58 配置服务器选项之三

8.4.2 配置网络隔离策略

“网络策略和访问”角色安装完成后，默认没有启用任何强制策略。本例中部署强制使用 DHCP 策略完成对客户端计算机的监控，没有通过安全验证的计算机将被隔离到非正常状态的网络区域中，得到“Error.book.com”DNS 域名，在没有部署更新服务器的环境中，将不能连接到域控制器或者其他应用服务器中，只能连接到网络策略服务器中。

1. 配置网络隔离策略

第 1 步，以域用户身份登录到网络策略服务器，选择“开始”→“管理工具”→“网络策略服务器”选项，显示如图 8-59 所示的“网络策略服务器”窗口。

第 2 步，单击“配置 NAP”超链接，启动“配置 NAP”向导，显示如图 8-60 所示的“选择与 NAP 一起使用的网络连接方法”对话框。

- ① 在“网络连接方法”下拉列表框中，选择“动态主机配置协议（DHCP）”选项。
- ② 在“策略名称”文本框中，输入策略的名称，该名称需要具备唯一性。

第 3 步，单击“下一步”按钮，显示如图 8-61 所示的“指定 NAP 强制服务器运行 DHCP 服务器”对话框。如果 DHCP 服务器和网络策略服务器不再同一台计算机中，需要设置 DHCP 服务器。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

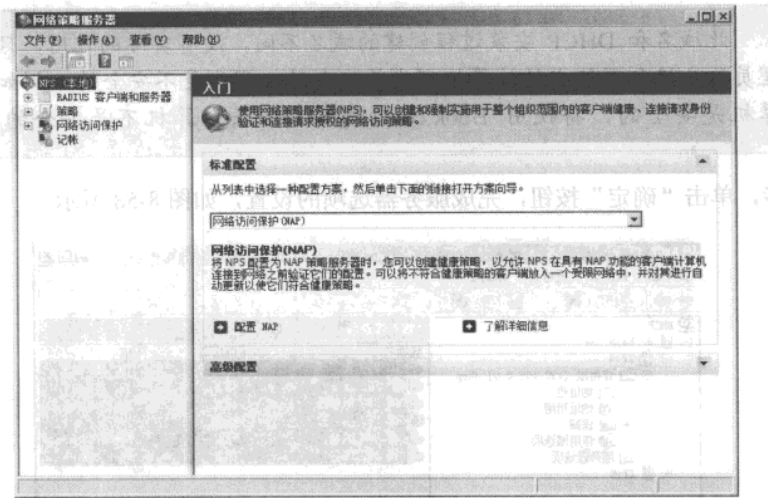


图 8-59 配置网络隔离策略之一

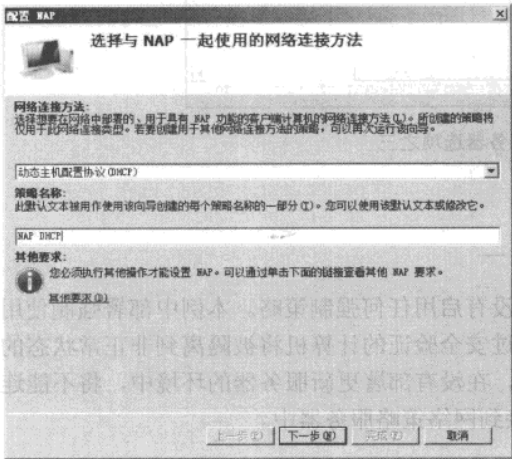


图 8-60 配置网络隔离策略之二

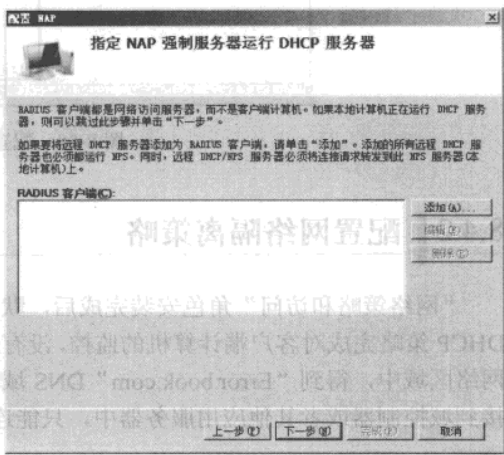


图 8-61 配置网络隔离策略之三

- ① 单击“添加”按钮，显示如图 8-62 所示的“新建 RADIUS 客户端”对话框，设置 DHCP 服务器。
- ② 在“友好名称”文本框中输入标识名称。
- ③ 在“地址”文本框中输入 DHCP 服务器的 IP 地址或者 DNS 名称。
- ④ 在“共享机密”区域设置 RADIUS 服务器和客户端计算机之间的通信密钥，根据情况设置即可，如图 8-63 所示。
- ⑤ 单击“确定”按钮，完成 DHCP 服务器的设置，如图 8-64 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

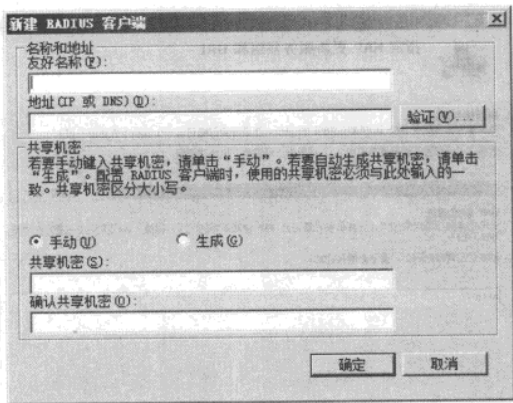


图 8-62 “新建 RADIUS 客户端”对话框

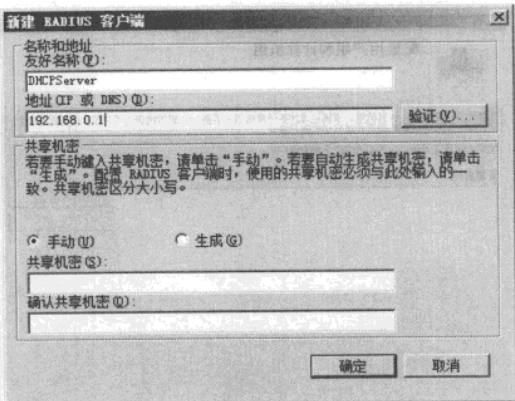


图 8-63 “新建 RADIUS 客户端”对话框

第 4 步，单击“下一步”按钮，显示如图 8-65 所示的“指定 DHCP 作用域”对话框。设置 DHCP 服务器的作用域，可以在“配置 NAP”向导完成后配置，本例中将不配置 DHCP 作用域。

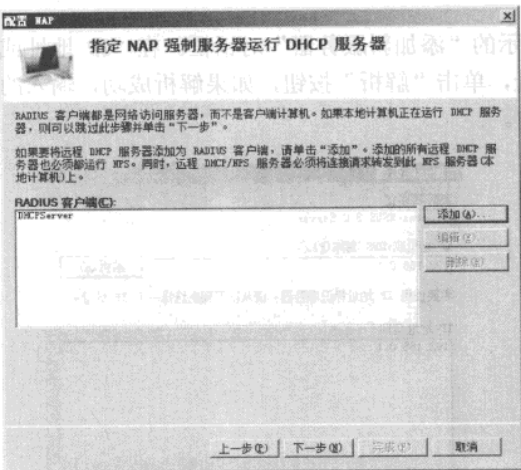


图 8-64 “指定 NAP 强制服务器运行 DHCP 服务器”对话框

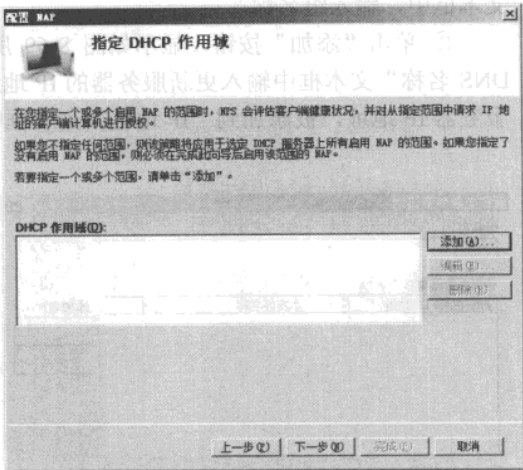


图 8-65 配置网络隔离策略之四

第 5 步，单击“下一步”按钮，显示如图 8-66 所示的“配置用户组和计算机组”对话框。设置需要监控的目标用户和计算机，如果不设置目标用户和计算机，则监控网络中的所有计算机和用户。

第 6 步，单击“下一步”按钮，显示如图 8-67 所示的“指定 NAP 更新服务器组和 URL”对话框。更新服务器组提供被隔离的用户和计算机自动完成修复功能的目标服务器组，URL 设置提示用户和计算机如何完成修复任务，以及提供相关的资源。

网管天下 网管经验谈

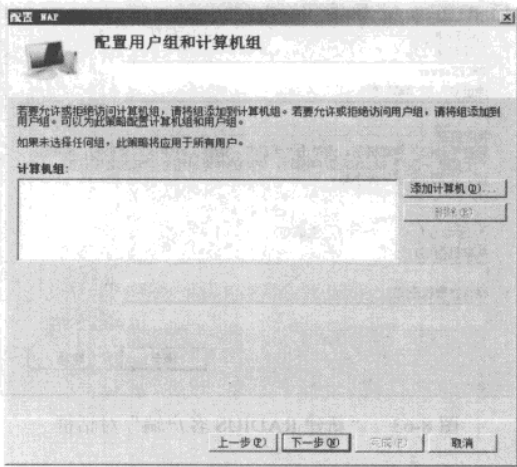


图 8-65 配置网络隔离策略之五

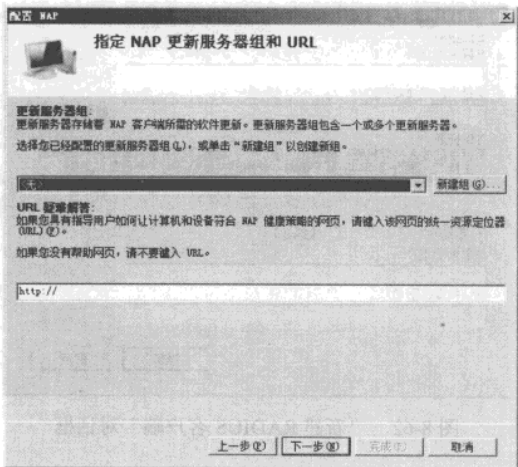


图 8-67 配置网络隔离策略之六

- ① 单击“新建组”按钮，显示如图 8-68 所示的“新建更新服务器组”对话框。在“组名”文本框中，输入组名称。
- ② 单击“添加”按钮，显示如图 8-69 所示的“添加新服务器”对话框。在“IP 地址或 DNS 名称”文本框中输入更新服务器的 IP 地址，单击“解析”按钮，如果解析成功，输入的服务器 IP 地址，被添加到“IP 地址”列表框中。

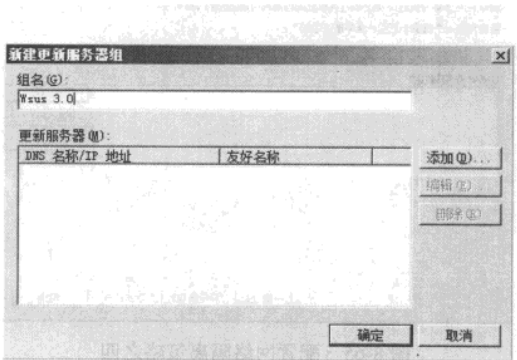


图 8-68 设置更新服务器之一

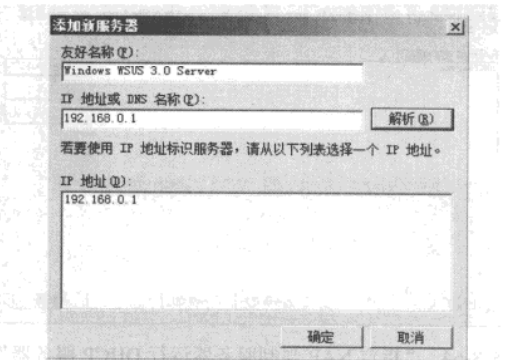


图 8-69 设置更新服务器之二

- ③ 单击两次“确定”按钮，完成更新服务器的设置，如图 8-70 所示。
- 第 7 步，单击“下一步”按钮，显示如图 8-71 所示的“定义 NAP 健康策略”对话框。NPS 服务部署完成后，已经安装“Windows 安全健康验证程序”，选择即可。选择“启用客户端计算机的自动更新”复选框，如果不选择该选项，则客户端计算机将不能自动或者修复停止的策略或者服务。被隔离的客户端计算机仅具备“拒绝对不具有 NAP 功能的客户端计算机的完全网络访问权限。只允许访问受限网络”功能，即被隔离的客户端计算机在没有指定“更新服务器组”的情况下，只能访问网络策略服务器，不能连接到其他服务器。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

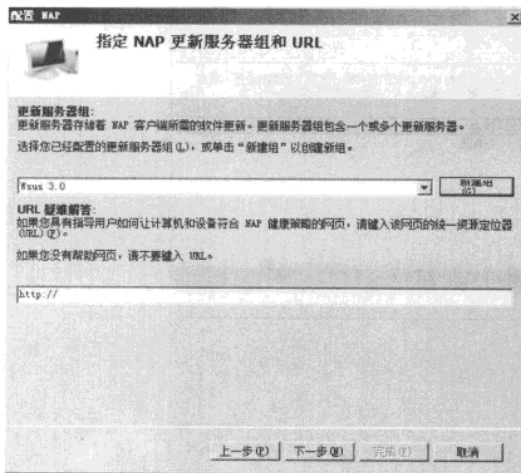


图 8-70 置更新服务器之三

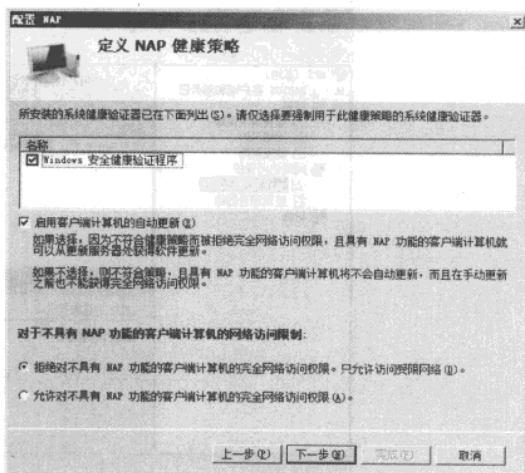


图 8-71 配置网络隔离策略之七

第 8 步，单击“下一步”按钮，显示如图 8-72 所示的“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框。

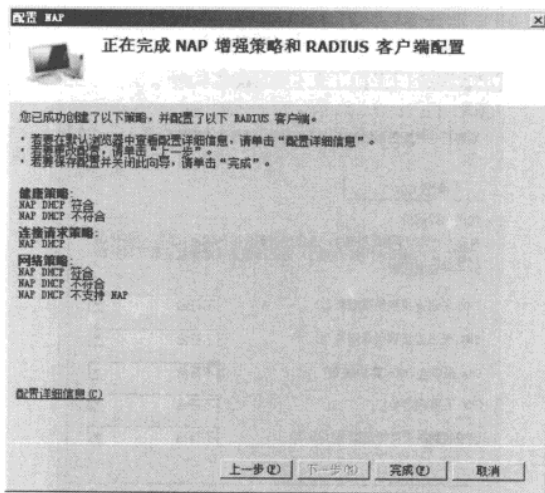


图 8-72 配置网络隔离策略之八

第 9 步，单击“完成”按钮，关闭“配置 NAP”向导，完成管理的策略配置。

2. 部署客户端计算机验证策略

在网络策略服务器中，更新系统健康验证器，为客户端计算机启用验证策略，验证策略包括：防火墙、病毒防护、间谍软件防护和自动更新策略。

第 1 步，打开“网络策略服务器”窗口，选择“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项，如图 8-73 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

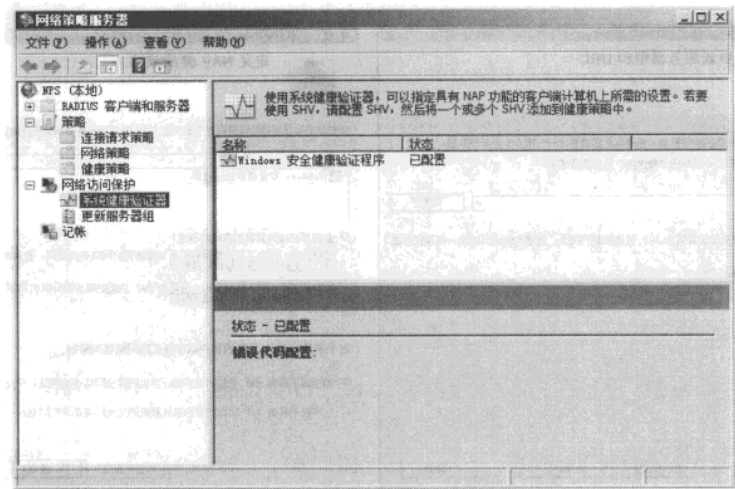


图 8-73 部署客户端计算机验证策略之一

第 2 步，右击“Windows 安全健康验证程序”选项，在弹出的快捷菜单中选择“属性”命令，打开“Windows 安全健康验证程序 属性”对话框，如图 8-74 所示。

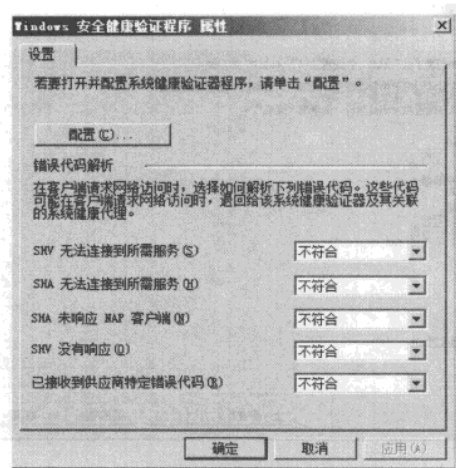


图 8-74 部署客户端计算机验证策略之二

第 3 步，单击“配置”按钮，显示如图 8-75 所示的“Windows 安全健康验证程序”对话框。在“Windows Vista”选项卡中，选择需要启用的验证策略。

第 4 步，切换到“Windows XP”选项卡，在“Windows XP”选项卡中选择目标验证策略，如图 8-76 所示。

第 5 步，单击多次“确定”按钮，完成系统健康验证程序的设置。

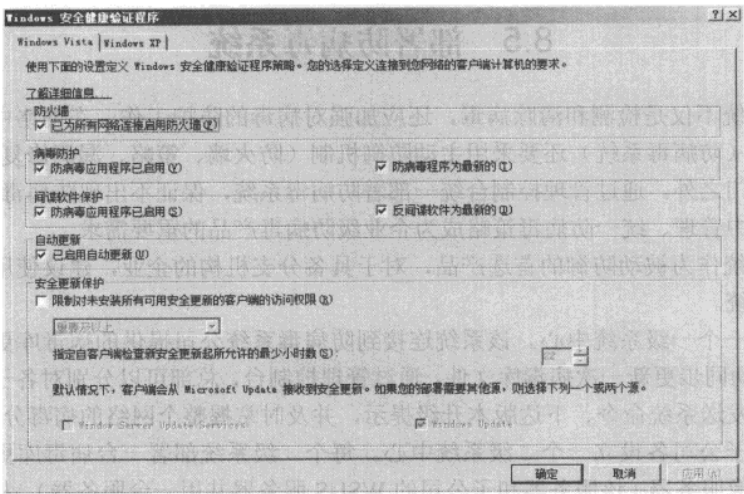


图 8-75 部署客户端计算机验证策略之三

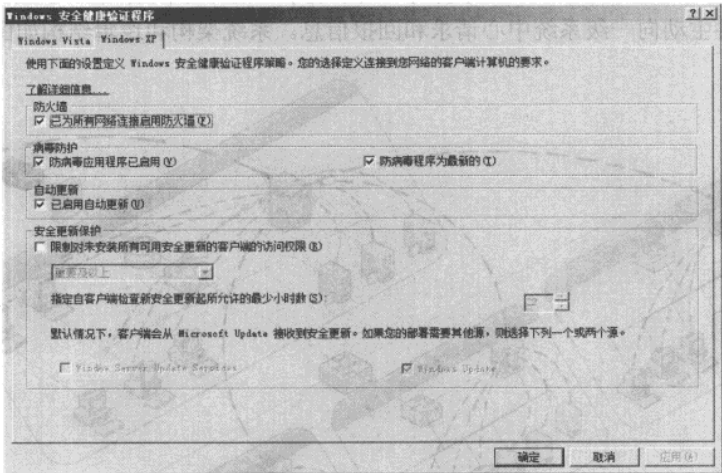


图 8-76 部署客户端计算机验证策略之四

3. 部署客户端计算机验证策略

Windows Server 2008 提供的网络访问保护功能，支持 Windows Vista、Windows XP SP3 和 Windows Server 2008 操作系统，在上述操作系统中已经集成了“Network Access Protection Agent”服务，默认情况下该代理服务没有启动。本例中使用组策略创建一条全局性的策略，使用组策略管理控制台启动以下策略。

- 启动“Network Access Protection Agent”服务。
- NAP 客户端计算机强制启用“DHCP 隔离强制客户端”策略。
- 启动“启用安全中心（仅限域）”策略。

8.5 部署防病毒系统

防病毒系统不仅是检测和清除病毒，还应加强对病毒的防护工作，在网络中不仅要部署被动防御体系（防病毒系统）还要采用主动防御机制（防火墙、策略、漏洞修复等），将病毒隔离在网络大门之外。通过管理控制台统一部署防病毒系统，保证不出现防病毒漏洞。因此，远程安装、集中管理、统一防病毒策略成为企业级防病毒产品的重要需求。

防病毒系统作为被动防御的首选产品，对于具备分支机构的企业，建议使用如下架构部署该防病毒系统。

总部设立一个一级系统中心。该系统连接到防病毒系统公司提供的病毒库更新站点服务器，每小时自动同步更新一次病毒库文件。通过管理控制台，总部可以分别对各子公司的服务器端和客户端发送系统命令、下达版本升级提示，并及时掌握整个网络的病毒分布情况等。

分别在各子公司各设立一个二级系统中心。每个二级系统部署一台病毒库更新服务器，或者称之为镜像服务器（该服务器和子公司的 WSUS 服务器共用一台服务器），从一级系统中心每小时同步更新一次病毒库。各子公司通过自己建立的二级系统中心对自己所管辖的全部计算机进行实时监控和病毒处理，并且对收到一级系统中心的命令做出相应处理措施，也可以管理本级系统，并主动向一级系统中心请求和回报信息。系统架构和逻辑结构如图 8-77 所示。

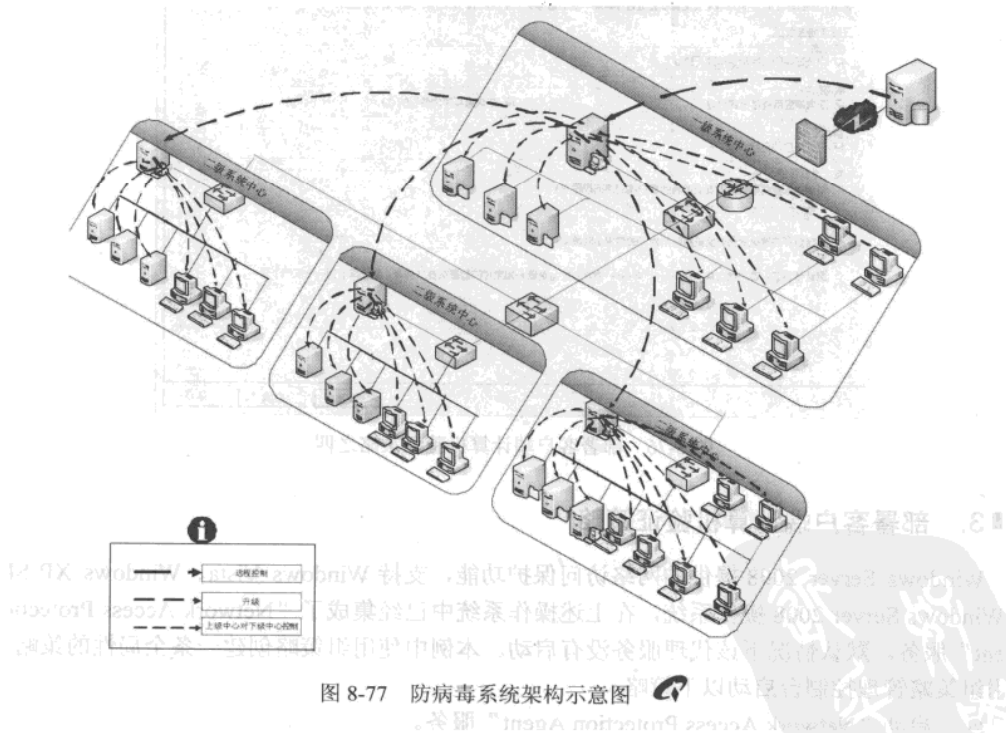


图 8-77 防病毒系统架构示意图

第9章 用户、计算机账户管理

网络管理在管理什么呢？除了硬件设备之外，管理员大部分时间管理目标是域用户和计算机。尤其是用户，用户是计算机使用者登录到网络的身份证，访问网络资源的有效证件。计算机账户从日常管理来说，很少用到，但却是标识计算机在网络中的身份证，如果计算机没有身份证，即使具备用户和访问权限，也不能从该计算机登录到网络中。本章中的用户指的是域用户，域指的是 Windows 的 Active Directory 活动目录。

9.1 组织单位管理

组织单位是个比较抽象的概念，举例来说：一座完整的大楼，大楼是 Active Directory 数据库，楼层是组织单位，房间是用户、计算机账户等域对象，每个楼层可以包含多个房间，就像每个组织单位中包含多个域对象。因此合理的使用组织单位，能够充分发挥“分层负责、授权自治”的优点，若能善用组织单位，使尽量避免形成多域架构，节省企业管理成本。

9.1.1 组织单位和组的区别

首先需要确认的是，组织单位和组是截然不同的目标组合。

组织单位和组都是域的一种对象。组织单位如同屋子，当同一个人在屋子里面时，这个人就不可能在商场，或者公园中。也就是说，一个人在一个组织单位中时，就不可能在洽谈组织单位中。

组标识用户具备的权利和权限，用户可以在不同组中，将具备不同的权限，用户所具备的权限就是所有不同的组的权限的交集。

组织单位是体现管理架构，而组是权利和权限的集合。

9.1.2 组织单位规划

从企业角度分析，可以按部门把所有的用户和设备组成层次架构，也可以按地理位置形成层次架构，还可以按功能和权限分成多个组织单位层次架构。组织单位具有很清楚的层次架构，并且支持嵌套功能，这种架构可以使管理者把组织单位切入到域中以反应出企业的组织架构并且可以委派任务与授权。

由于组织单位层次架构局限于域的内部，所以一个域中的组织单位层次架构与另一个域中的组织单位层次架构没有任何关系。因此，一个企业有可能只用一个域来构造企业网络，这时候就可以使用组织单位来对对象进行分组，形成多种管理层次架构，从而极大地简化网络管理工作。组织中的不同部门可以成为不同的域，或者一个组织单位，从而采用层次化的命名方法来反映组织架构和管理授权。根据组织架构进行细化的管理授权可以解决很多管理上的

网管天下 网管经验谈

问题，在加强中央管理的同时，又不失机动灵活性。

1. 基本原则

设计组织单位架构时，基本原则是简单性+适用性=可持续性。如果设计过于简单，则它可能并不适用，因此将不得不过于频繁地进行更改。如果设计适用性过强，则所有内容都将被分类，这会使情况变得过于复杂。

2. 不合理的规划

计划欠佳的组织单位架构往往会我行我素，如果在目录中创建了一个新对象，但管理员不知道将其置于组织单位架构中的什么位置，只能选择要么创建一个新组织单位，要么将该对象放在某个不相干的位置。这两种情况都比较危险。创建一个新组织单位很容易做到，但从长远角度来看很难进行跟踪。如果将某个对象添加到与其不相干的现有组织单位中，则此新对象可能会接收它不应获得的策略，或者该对象的权限可能被委派给非目标用户。

3. 全局衡量

过度强调阻止单位架构可能忽略域设计的其他方面，例如规划站点拓扑或考虑域控制器大小。另一方面，如果组织单位规划不受重视，组策略和委派功能将会受到影响。可能部分管理员认为组织单位架构很灵活，如果不合适之后可以进行更改，管理员通常发现后期更改组织单位架构要比原来预期的困难，可以添加新的组织单位，但是旧的组织单位很难清理干净。

4. 组织单位规划

组织单位必须能够反映企业架构的细节，可以建立组织单位来减少对那些小型的使用者、群组、资源的管理控制。管理控制的授权可以是完全的（能建立使用者、更改密码、管理账户原则等），也可以是有限的（只能更改密码）。因为最高层的组织单位可以包含其他层级的组织单位，因此如果需要的话应尽可能地将细节延伸到各层级。应该将这些对象纳入与工作和组织相符的逻辑架构中。

利用组织单位能避免使用者由企业层级的网络管理员进行管理，执行诸如建立计算机账户、设定密码等，有效的方式为提供组织单位层级的管理，将网络管理员从琐碎的工作中解脱出来。通过限制对发布资源的授权访问，使用者将只能看到已被授权存取的对象。除非父域和父组织单位的安全性原则被指定不能使用，否则组织单位将继承它们。

为企业建立组织单位时遵循以下原则：

- 建立组织单位进行授权管理。
- 建立一个逻辑性、有意义的组织单位架构，该架构可以使组织单位管理员有效率地完成工作。
- 建立组织单位来应用安全性原则。
- 建立组织单位来提供或限制特定使用者对发布资源的可见度。
- 建立稳定的组织单位架构。组织单位也为企业名称空间的弹性以适应企业的变更需求。
- 避免向任一组织单位分配过多的子对象。

在开始设计组织单位架构之前，切记必须先建立分层、统一、稳定且其通用程度足以保

证企业的任一部门都可以使用的组织单位和对象名称，还应该尽量避免组织单位有过多的子对象。

为第一层级建立组织单位架构的一个方法是命名最顶层的组织单位，使之成为能明确定义下面组织单位根。另一种建立一致性组织单位架构的方法是判断对象的层级来建立。一旦将对象细分成各个群组之后，就可以为它们附上适宜的顶层组织单位名称。

5. 管理架构

决定组织单位架构所依靠的划分依据十分重要，许多网络管理员都将域架构建立成能反映其企业行政架构的模式，实际的架构应该根据企业的业务级别，以及功能模式综合架构。下面介绍划分组织单位分层时各种不同的方法。

（1）管理架构。

通过管理对象建立组织单位架构时，对该组织单位的管理员来说十分便利。在域中，可以建立以对象为基础的组织单位，如用户群、计算机群、应用程序群、打印机、安全性原则（例如软件限制策略）等。以逻辑性、有意义的方式建立之组织单位能有助于管理员快速、容易地完成发布策略。在大多数情况下，这是组织组织单位的最佳架构方式，可以确保变动的数目会减至最低。管理架构如图 9-1 所示。

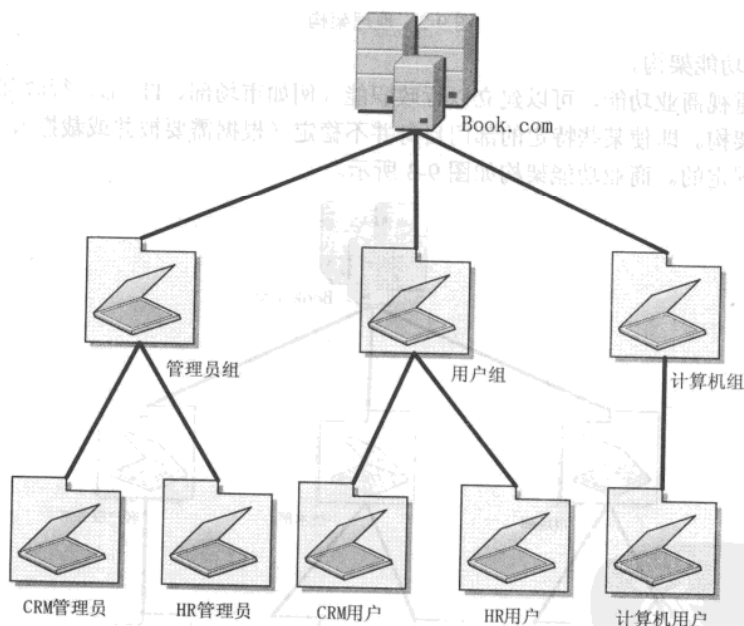


图 9-1 管理架构

（2）地理架构。

如果公司分布不同的地理位置，以地理位置为基础创建组织单位，将是理想的架构。根据不同的地理位置为每个组织单位指派管理员和发布策略，为组织单位的管理员赋予更大的权利。地理架构如图 9-2 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

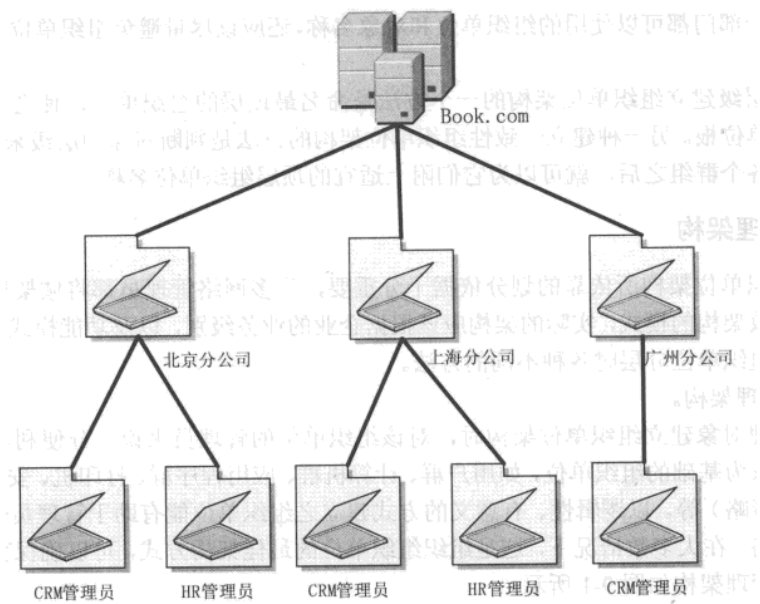


图 9-2 地理架构

(3) 商业功能架构。

如果公司重视商业功能，可以建立以行政职能（例如市场部、IT 部、行政部）部门为基础的 organizational unit structure。即使某些特定的部门自身并不稳定（根据需要被并或裁撤），但对这些功能的需求却是固定的。商业功能架构如图 9-3 所示。

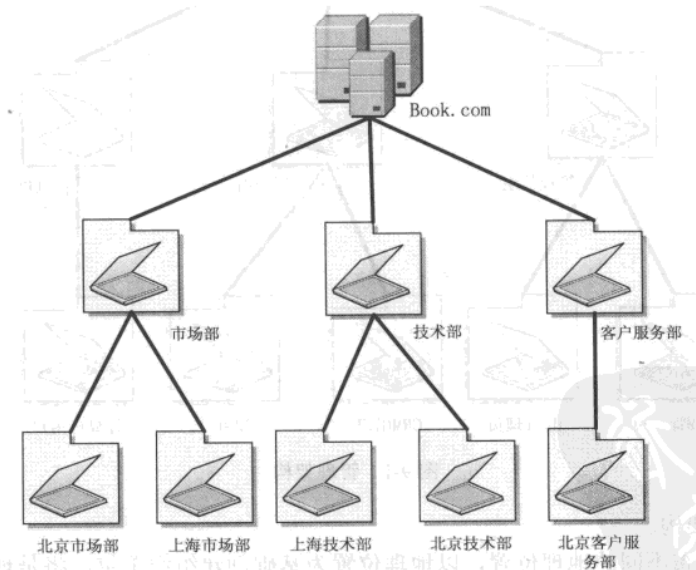


图 9-3 商业功能架构

(4) 部门架构。

以行政职能部门为原则创建的 organizational unit structure，该原则能与当前行政组织架构相互对应，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

但当行政组织架构重组时将遇到困难。部门架构如图 9-4 所示。

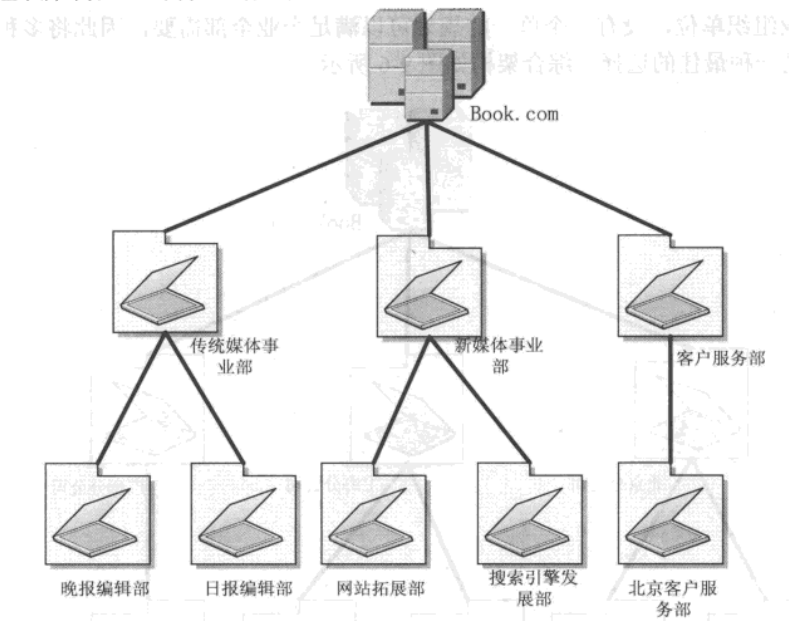


图 9-4 部门架构

(5) 项目架构。

使用此架构的组织单位模式以项目和成本中心为基础，而非以部门或者地理位置划分。如果企业的业务通过项目推动，例如软件开发工程，外包业务等。这并不是一个值得建议的组织单位架构，因为它经常变动。项目架构如图 9-5 所示。

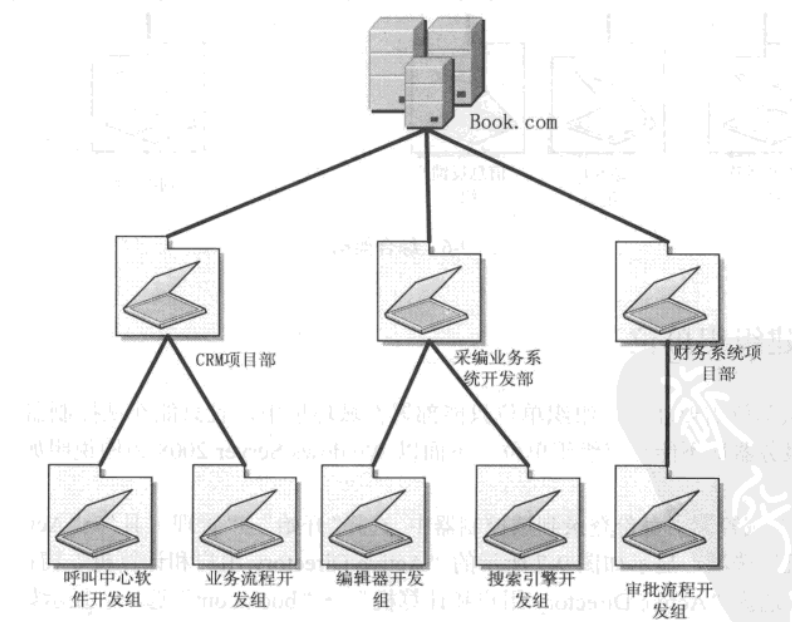


图 9-5 项目架构

网管天下 网管经验谈

(6) 综合架构。

规划企业组织单位，没有一个单一的规划可以满足企业全部需要，因此将多种架构结合起来，应该是一种最佳的选择。综合架构如图 9-6 所示。

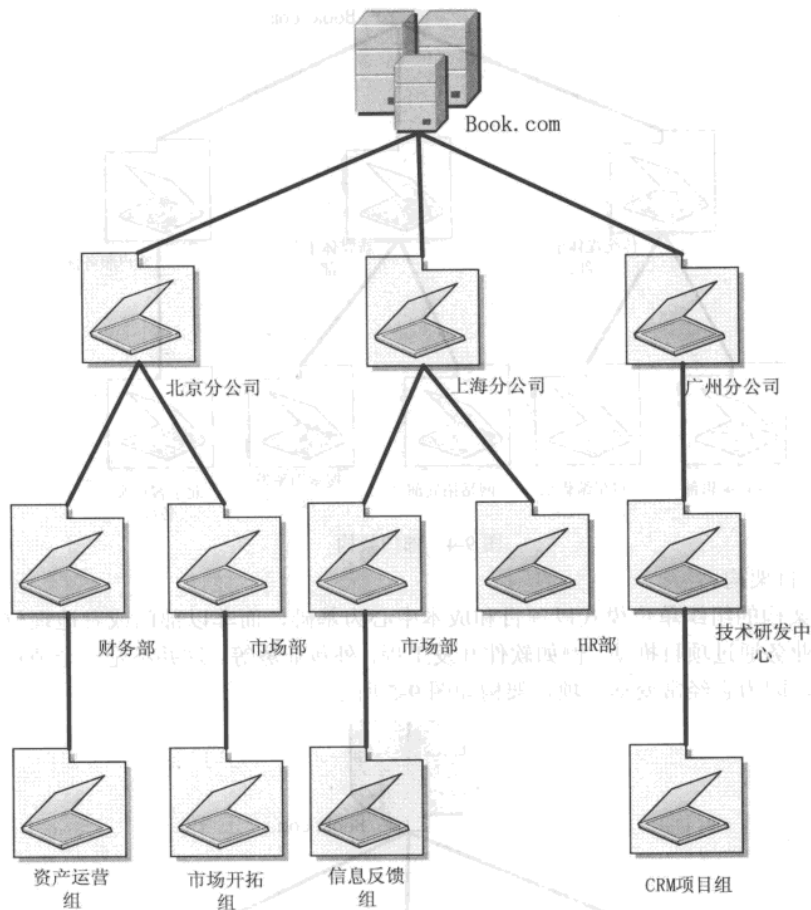


图 9-6 综合架构

9.1.3 创建组织单位

创建组织单位需要注意，组织单位只能部署在域环境中，且只能在域控制器中，成员服务器、独立服务器均不能部署组织单位。下面以 Windows Server 2008 为例说明如何创建组织单位。

第 1 步，以域管理员身份登录到域控制器中。选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，显示如图 9-7 所示的“Active Directory 用户和计算机”窗口。

第 2 步，选择“Active Directory 用户和计算机”→“book.com”选项，显示如图 9-8 所示的“Active Directory 用户和计算机”窗口。

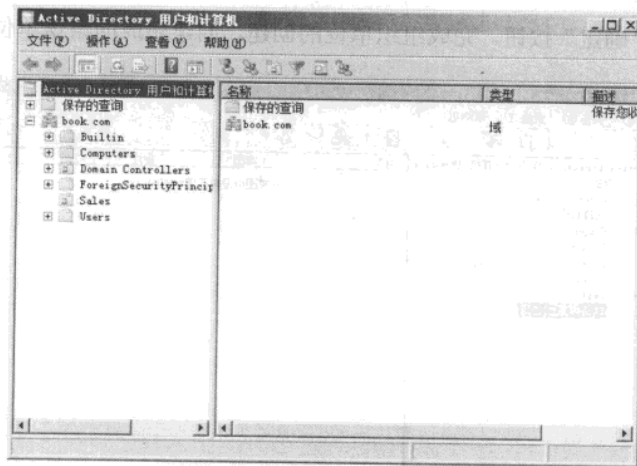


图 9-7 创建组织单位之一

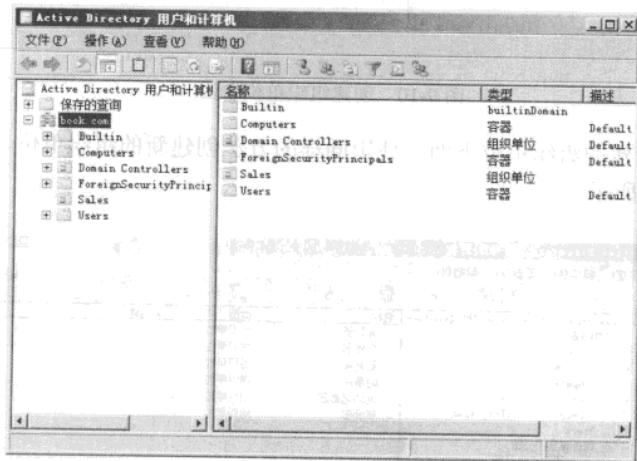


图 9-8 创建组织单位之二

第 3 步，右击“book.com”选项，在弹出的快捷菜单中选择“新建”选项，在弹出的级联菜单中选择“组织单位”命令，显示如图 9-9 所示的“新建对象—组织单位”对话框。在“名称”文本框中，输入组织单位的名称。

提示 如果选择“防止容器被意外删除”复选框，则新建的组织单位将不能被移动和删除，即使“Domain Admins”组成员也不能删除。如果不选择此功能，则可以正常删除和移动组织单位。

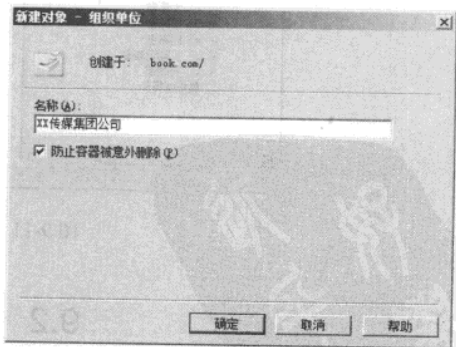


图 9-9 创建组织单位之三

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

第 4 步，单击“确定”按钮，完成组织单位的创建，创建完成的组织单位如图 9-10 所示。

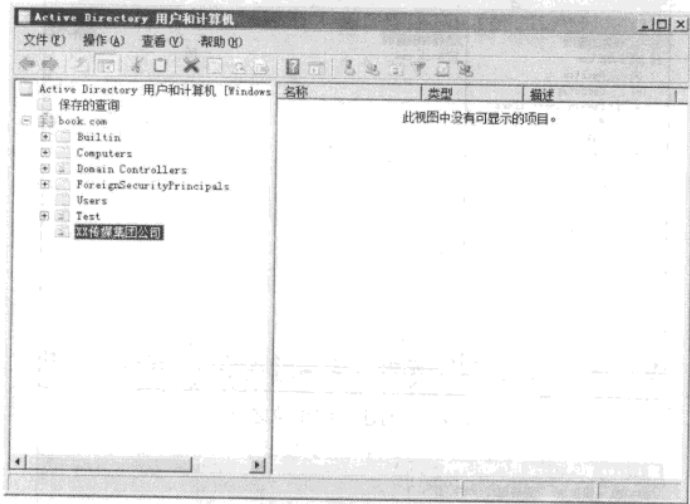


图 9-10 创建组织单位之四

第 5 步，在新建的组织单位下面，使用同样的方法创建新的组织单位，创建完成的组织单位架构如图 9-11 所示。

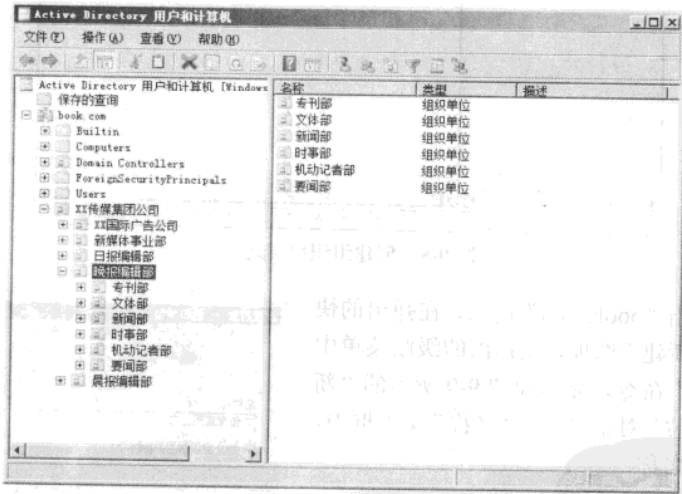


图 9-11 创建组织单位之五

9.2 组 管 理

组是一批具有相同管理任务的用户和计算机账户的集合，例如学校有英语教研组、数学教研组等，可以把教研组认为是域里的组，而老师可以认为是域里的一个对象。学校可以通过

划分教研组管理各个科目老师的教学，而域根据划分好的组，对域对象进行统一管理。

9.2.1 组分类

在 Windows Server 中，根据其组类型可以分为安全组（Security Group）和通信组（Distribution Group），根据其组作用域范围又可以分为全局组（Global Group）、域本地组（Domain Local Group）和通用组（Universal Group）。组的类型决定组可以管理哪些类型的任务，组作用域决定组的应用范围。

1. 安全组

顾名思义，安全组是用来设置有安全权限相关任务的用户或者计算机账户集合。安全组中的成员会自动继承其所属安全组的所有权限。使用安全组可以执行以下操作：

(1) 分配用户权限。

将用户权限分配给安全组，以确定该组成员在作用域内可执行的操作。在安装 AD DS 域服务时会自动将用户权限分配给某些安全组，并定义用户在域中的管理角色。例如，添加到“备份操作员”组的用户能够备份和还原域中各个域控制器上的文件和目录。

(2) 将资源权限分配给安全组。

资源权限确定可以访问共享资源的对象，并确定访问级别，例如“完全控制”权限，建议使用安全组来管理对共享资源的访问和权限。

(3) 发送电子邮件。

安全组具有分发组的全部功能，也可用做电子邮件实体。当向安全组发送电子邮件时，会将邮件发给安全组的所有成员。

2. 分发组

顾名思义，分发组是用于用户之间通信的组，使用分发组可以向一组用户发送电子邮件，分发组典型应用是 Microsoft Exchange Server 中的用户组，可以向一组用户发送电子邮件。

9.2.2 组作用域

Windows Server 2008 中，根据组作用域不同，可以分为：全局组、通用组、域本地组。

1. 全局组

全局组属于某个域，但是作用域是整个森林。全局组的成员只能是本地的域中的用户或者计算机账户，可以访问在森林任何域里的资源。全局组可以全局使用，即可在本域和有信任关系的其他域中使用，体现的是全局性。

全局组的作用域，只能在创建该全局组的域上添加用户、计算机账户和其他全局组，全局组可以嵌套在其他组中，支持全局组嵌套，即将某个全局组添加到同一个域上的另一个全局组中，或添加到同一个森林其他域的通用组和域本地组中（不能加入到同一个森林其他域的全局组中）。虽然可以利用全局组授予访问任何域资源的权限，但一般不直接用它来进行权限管理。

网管天下 网管经验谈

2. 通用组

通用组不属于任何域，通常用于域间访问。通用组的成员可以访问在森林任何域里的资源。通用组以从任何域中添加用户和组，可以嵌套于其他域组中。通用组存储在全局编录（GC）中，通用组名称必须在整个森林里是唯一的。由于 GC 中不仅包含通用组，还包含有通用组的成员信息，因此每次对通用组的修改（成员增加/删除），都会引发 GC 复制流量。所以，通用组的成员不要经常频繁地发生变化，否则会带来大量的复制流量。在 Active Directory 中的用户在登录时，需要向 GC 查询用户的通用组成员身份，所以在 GC 不可用时，活动目录中的用户有可能不能正常访问网络资源。

3. 域本地组

域本地组只能在本域的域控制器上使用，域本地组的成员只能访问本地的资源。本地域组可以从域添加用户、通用组和全局组。域本地组不能嵌套于其他组中，主要是用于授予访问本域资源权限。本地域组的成员可以包括 Windows Server 2003、Windows 2000 Server、Windows NT 和 Windows Server 2008 域中的其他组和账户，仅能在域内为这些组的成员分配权限。

4. 组类型更改

组有两种类型安全组和分发组，组类型之间可以相互转换。如果要更改组类型，必须是 AD DS 域服务中 Account Operators 组、Domain Admins 组或 Enterprise Admins 组的成员，或者被委派适当的权限。Windows Server 2008 的域功能级别设置为 Windows 2000 本机或更高。域功能级别被设置为 Windows 2000 混合时无法转换组。

5. 更改组作用域

创建新组时，在默认情况下新组配置为具有全局安全组，与当前域功能级别无关。域功能级别设置为 Windows 2000 本地以上的功能级别中，允许进行下列转换：

- 全局安全组到通用安全组，只有当要更改的组不是另一个全局的成员时，允许进行该转换。
- 本地域组到通用安全组，只有当要更改的组没有另一个“本地域组”作为其成员时，允许进行该转换。
- 通用安全组到全局安全组，只有当要更改的组没有另一个“通用组”作为其成员时，允许进行该转换。
- 通用安全组到本地域组，该操作没有限制。

9.2.3 组部署原则

Windows Server 2008 服务器操作系统中组功能十分强大，在部署资源访问时，建议遵守 AGDLP 和 AUDLP 原则。

1. 组中的用户规划

管理组的实质是对用户的管理，因此对组规划建议遵循以下原则：

- 相同部门的人在同一个组内。
- 将对于某个资源（打印机、共享文件夹访问等）具有相同使用权限的人员规划成同一个组。

2. 组规划

在单域网络中，“全局组”与本地域组配合使用，遵循以下原则：

- 将用户加入到“全局组”内。
- 将此“全局组”加入到“本地域组”内。
- 指派适当的权限给此“本地域组”。

3. 授权原则

对于资源（文件夹或打印机）的访问授权，建议使用“AGDLP”原则和“AUDLP”原则。

首先把用户（Account）加入到全局组（Global Group）或者通用组（Universal Group）中，然后把全局组加入到域本地组（Domain Local Ggroup，可以是本域或其他域的域本地组），最后对于域本地组进行授权（Permissions）。

“AGDLP”部署完成后，当给一个用户赋予某一个权限时，只要把这个用户加入到某一个全局组即可。

4. 应用实例

下面以案例的方式介绍 AGDLP 原则。在本公司中有两个域，TEST.COM 域和 BOOK.COM 域。TEST.COM 域中的 5 个财务人员和 BOOK.COM 域中的 3 个财务人员都需要访问 BOOK.COM 域中的“Software”文件夹。

（1）无原则规划。

在 BOOK.COM 域中建立一个“本地域组”，因为“本地域组”的成员可以来自所有的域，然后把这 8 个人都加入这个“本地域组”，并把“Software”文件夹的访问权赋给“本地域组”。

缺点：因为本地域组在 BOOK.COM 域中，所以管理权也在 BOOK.COM 域。如果 TEST.COM 域中的 5 个人变成 6 个人，只能是 TEST.COM 域管理员通知 BOOK.COM 域管理员，将“本地域组”的成员做一下修改，BOOK.COM 域的管理员没有管理的权利。

（2）AGDLP 规划。

在 TEST.COM 域和 BOOK.COM 域中都各建立一个“全局组”（G），在 BOOK.COM 域中建立一个“本地域组”，把这两个“全局组”都加入 BOOK.COM 域中的“本地域组”中，把“Software”文件夹的访问权赋给“本地域组”。两个“全局组”都有权访问“Software”文件夹。

优点：对多域环境，分而治之。两个“全局组”分布在 TEST.COM 域和 BOOK.COM 域中，也就是 TEST.COM 域和 BOOK.COM 域的管理员都可以自己管理自己的“全局组”，只要把那 5 个人和 3 个人分别加入“全局组”中，就可以访问“Software”文件夹。如果需要添加添加用户或者其他任何修改，由各自域的管理员独立完成。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2.4 常用组管理任务

1. 创建组

创建“本地域组”、“安全组”和“通用组”操作过程完全相同，以创建“全局组”为例说明。

第1步，以域管理员身份登录域控制器，选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口，选择“book.com”→“北京分公司”选项，如图 9-12 所示。

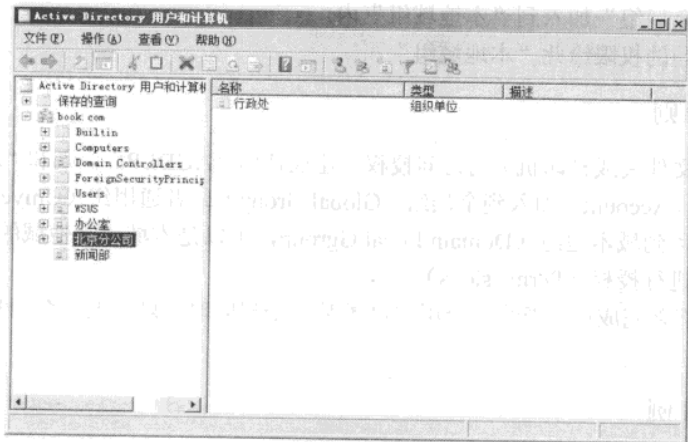


图 9-12 创建组之一

第2步，右击“北京分公司”，在弹出的快捷菜单中选择“新建”选项，在弹出的级联菜单中选择“组”命令，或者单击菜单栏中的“操作”菜单，在弹出的下拉菜单中，选择“新建”选项，在弹出的级联菜单中选择“组”命令，如图 9-13 所示。

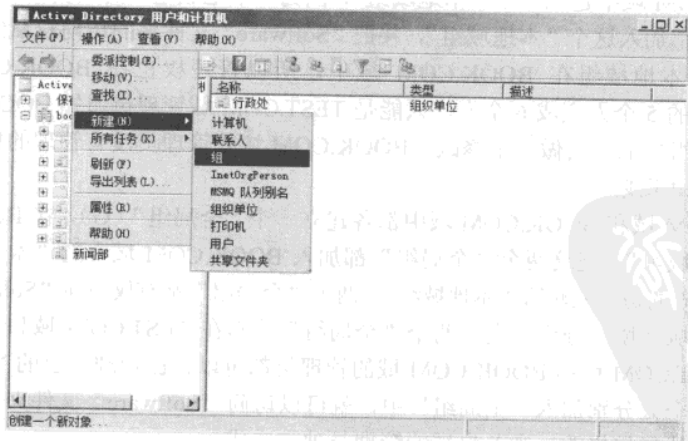


图 9-13 创建组之二

用户、计算机账户管理 9

第 3 步，命令执行后，显示如图 9-14 所示的“新建对象一组”对话框，在“组名”文本框中，输入组在当前域中唯一名称。在“组作用域”区域中，选择“全局”单选按钮。在“组类型”区域中，选择“安全组”单选按钮。

第 4 步，单击“确定”按钮，完成新组的创建，如图 9-15 所示。

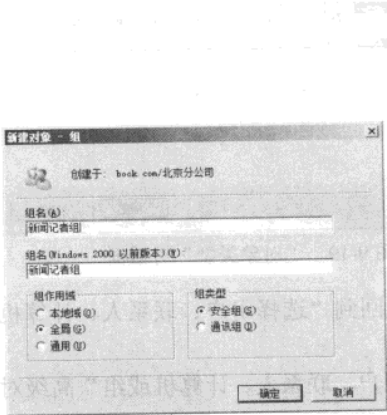


图 9-14 创建组之三

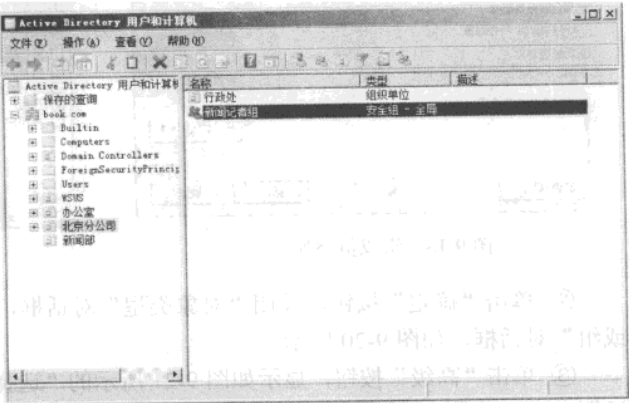


图 9-15 创建组之四

2. 嵌套组

组嵌套，一个组是另外一个组的子集，即一个组包容其他的组。嵌套组可以包容多个组，如果包容的组包含其他组，则权限自动继承到包含的组中。

第 1 步，打开“Active Directory 用户和计算机”窗口，选择“book.com”→“新闻部”选项，右击“新闻记者组”，在弹出的快捷菜单中选择“属性”命令，显示如图 9-16 所示的“新闻记者组属性”对话框。

第 2 步，切换到“成员”选项卡，显示如图 9-17 所示的“成员”对话框。

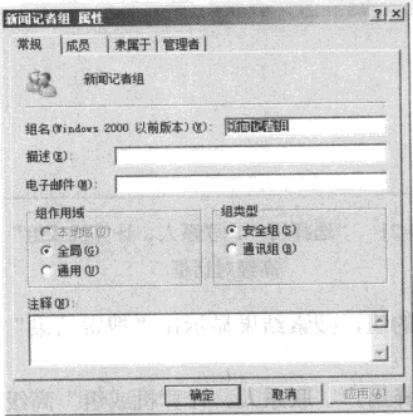


图 9-16 组成员添加之一

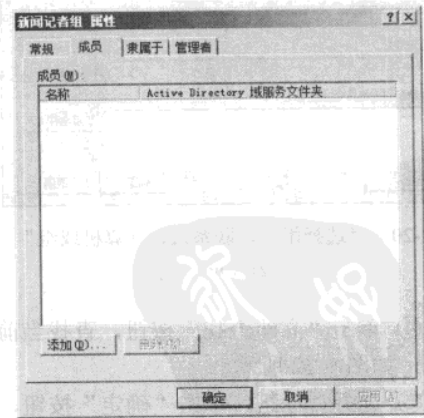


图 9-17 组成员添加之二

第 3 步，单击“添加”按钮，显示如图 9-18 所示的“选择用户、联系人、计算机或组”

网管天下 网管经验谈

对话框。

① 单击“对象类型”按钮，显示如图 9-19 所示的“对象类型”对话框。在“对象类型”列表框中，仅选择“组”复选框即可。

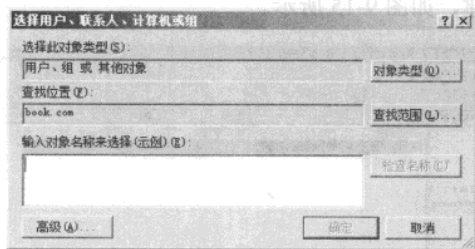


图 9-18 组成员添加之三

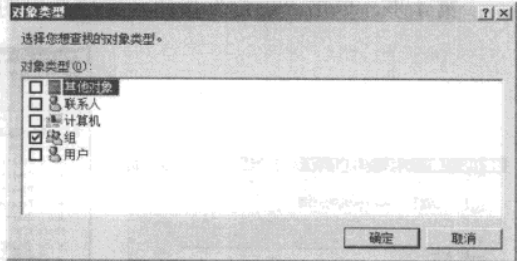


图 9-19 “对象类型”对话框

② 单击“确定”按钮，关闭“对象类型”对话框，返回到“选择用户、联系人、计算机或组”对话框，如图 9-20 所示。

③ 单击“高级”按钮，显示如图 9-21 所示的“选择用户、联系人、计算机或组”高级对话框。

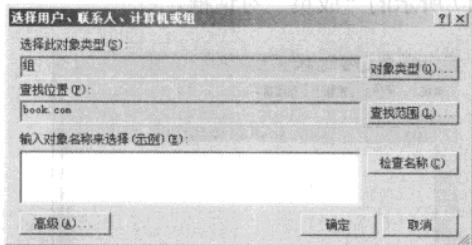


图 9-20 “选择用户、联系人、计算机或组”对话框

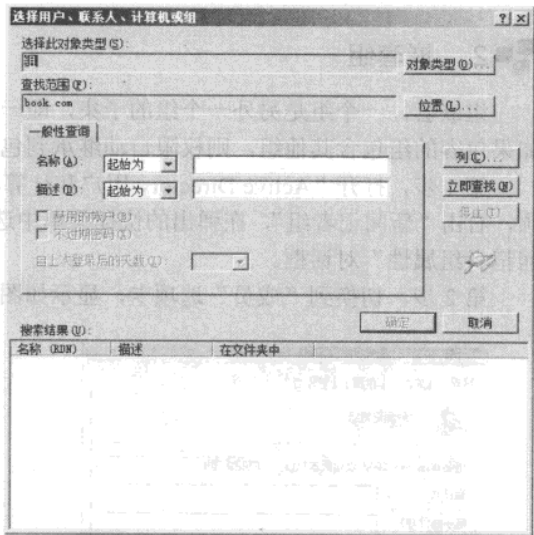


图 9-21 “选择用户、联系人、计算机或组”高级对话框

④ 单击“立即查找”按钮，查找当前域中可用的组，搜索结果显示在“搜索结果”列表框中，如图 9-22 所示。

⑤ 选择目标组，单击“确定”按钮，关闭“选择用户、联系人、计算机或组”高级对话框，返回到“选择用户、联系人、计算机或组”对话框，如图 9-23 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

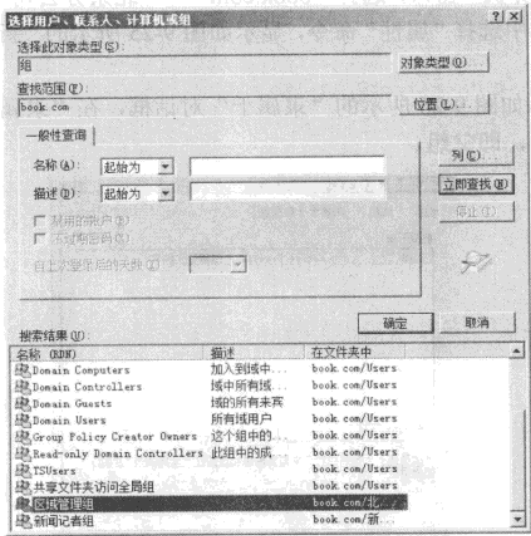


图 9-22 “选择用户、联系人、计算机或组”高级对话框

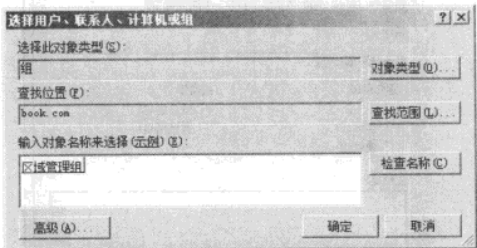


图 9-23 “选择用户、联系人、计算机或组”对话框

⑥ 单击“确定”按钮，关闭“选择用户、联系人、计算机或组”对话框，返回到“新闻记者组属性”对话框，在“成员”列表中显示添加的成员，如图 9-24 所示。

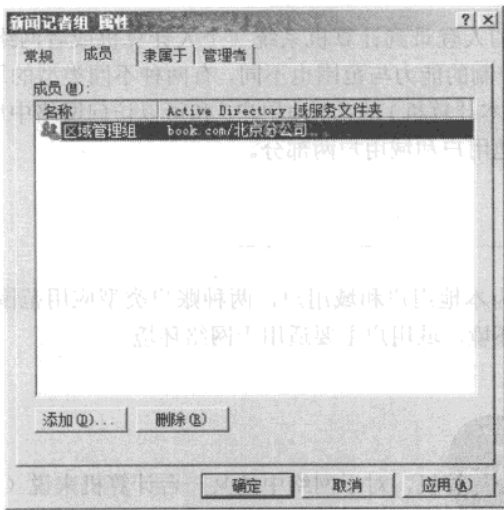


图 9-24 “新闻记者组属性”对话框

第 4 步，单击“确定”按钮，完成组嵌套。

3. 查看组隶属关系

组之间可以嵌套，一个组可以隶属于多个组，下面介绍如何查看组的隶属关系。

网管天下 网管经验谈

第 1 步，打开“Active Directory 用户和计算机”窗口，选择“book.com”→“北京分公司”选项，右击“新闻记者组”，在弹出的快捷菜单中选择“属性”命令，显示如图 9-25 所示的“新闻记者组”对话框。

第 2 步，切换到“隶属于”选项卡，显示如图 9-26 所示的“隶属于”对话框，在“隶属于”文件列表框中，显示选择的组所隶属的组，即父组。

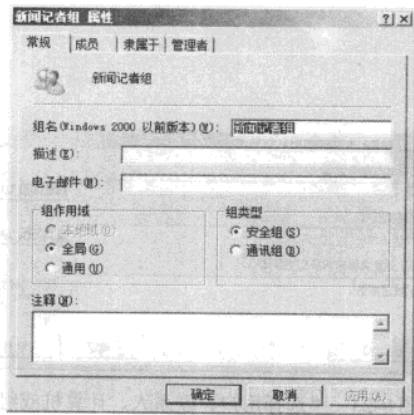


图 9-25 组隶属关系之一

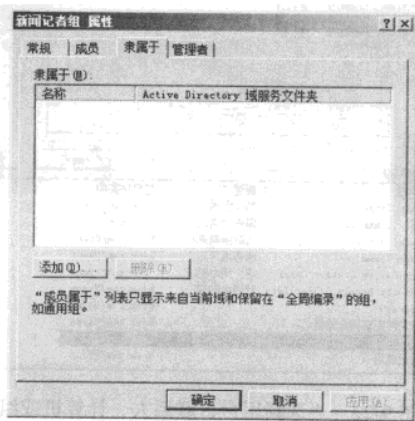


图 9-26 组隶属关系之二

9.3 用户管理

用户是使用计算机的人登录到计算机系统（个人计算机或者网络）的身份。用户的权限不同，对计算机及网络控制的能力与范围也不同。有两种不同类型的用户：能访问本地计算机（或使用远程计算机访问本计算机）的“本地用户”和可以访问网络中所有计算机的“域用户”。计算机中的用户分为本地用户和域用户两部分。

9.3.1 注意事项

计算机中的用户分为本地用户和域用户，两种账户类型应用范围不同。本地用户主要只用于工作组环境和个人环境，域用户主要适用于网络环境。

1. 用户分类

(1) 本地用户。

本地用户针对某一台计算机，对于网络中的某一台计算机来说（域控制器除外），每台计算机都可以创建若干个“本地用户”，使用这些创建的“本地用户”就可以使用（或通过远程访问）这台计算机。使用“本地用户”只能访问某一台计算机，不同的计算机有不同的本地用户。

(2) 域用户。

“域用户”在网络中的域控制器上创建，使用“域用户”可以（根据权限）访问网络中的所有计算机或某些计算机。

2. 用户的作用

当企业的员工要从自己的计算机登录到域时，该员工必须有一张被域控制器认可的“身份证”，这张身份证在域中就是用户。在域中创建和管理用户的操作必须在域控制器中进行。

用户的用途主要用于：

- 验证用户或计算机的身份：用户使用户能够利用经域验证后的标识登录到计算机和域。登录到网络的每个用户应有自己的唯一账户和密码。为了获得最高的安全性，应避免多个用户共享同一个账户。
- 授权或拒绝访问域资源：一旦用户已经过身份验证，那么就可以根据指派给该用户的关于资源的显式权限，授予或拒绝该用户访问域资源。
- 管理其他用户：在本地域中可以使用委派控制，允许对某个用户进行单独的权限委派，例如：使某个用户具备更改其他用户密码的权限。
- 审核使用用户或计算机账户执行的操作：审核有助于监视账户的安全性。

3. 用户附属属性

每个域用户都有许多账户选项，这些选项将确定如何对使用该特定用户登录网络的人员进行身份验证，描述信息见附表 9-1 所示。

表 9-1 账户选项

账户选项	描述
用户下次登录时须更改密码	强制用户在下次登录网络时更改自己的密码，要确保该用户是知道密码的唯一人选时启用此选项
用户不能更改密码	防止用户更改自己的密码，要对用户（如 Guest 账户或临时账户）保持控制时启用此选项
密码永不过期	防止用户的密码过期，建议服务账户启用此选项并使用强密码。
用可还原的加密来储存密码	允许用户从 Apple 计算机登录到 Windows 网络，如果用户没有从 Apple 计算机登录，则不要启用此选项
账户已禁用	防止用户使用选定的账户进行登录，很多管理员使用已禁用的账户作为公用用户的模板
交互式登录必须使用智能卡	要求用户拥有智能卡才能以交互方式登录到网络。用户还必须具有连接到计算机的智能卡读卡器以及智能卡的有效个人标识号（PIN）。启用此选项时，会自动将用户的密码设置为随机而复杂的值，并设置“密码永不过期”账户选项
账户可以委派其他账户	允许在此账户下运行的服务代表网络上的其他用户执行操作。如果某项服务在可以委派其他账户的用户（也称服务账户）下运行，则可以模拟客户端访问正在运行该服务的计算机上的资源或其他计算机上的资源
敏感账户，不能被委派	如果无法将账户（例如 Guest 或临时账户）分配给其他账户进行委派，则可以使用此选项
此账户需要使用 DES 加密类型	提供对数据加密标准（DES）的支持。DES 支持多个加密级别，包括 Microsoft 点对点加密（MPPE）标准（40 位）、MPPE 标准（56 位）、MPPE 强密码（128 位）、Internet 协议安全（IPsec）DES（40 位）、IPsec56 位 DES 和 IPsec 三重 DES（3DES）
不要求 Kerberos 预身份验证	提供对 Kerberos 协议备用实现的支持，但在启用此选项时请保持慎重，因为 Kerberos 预身份验证提供其他安全性，并要求客户端和服务端之间的时间同步

4. 用户具备权限

用户权限应用目标是操作。用户权限体现在对网络中资源访问权限的设置。用户必须获得明确的授权后才能访问资源，如果用户账号没有被授予权限，就不能访问相应的资源。为了控制用户对某个资源的访问，就必须指定权限。当然，也可以为某个用户设置拒绝权限。最

网管天下 网管经验谈

有代表性的权限应用就是 NTFS。常用的权限见附表 9-2 所示。

表 9-2 用户访问权限列表

权 限	允许用户完成的操作
读取	查看该文件夹中的文件和子文件夹 查看文件夹的所有者、权限和属性（如只读、隐藏、存档和系统）
写入	在该文件夹内新建文件和子文件夹 更改文件夹属性，查看文件夹的所有者和权限
列出文件夹目录	查看该文件夹中的文件和子文件夹的名称
读取及运行	包括“读取”权限和“列文件夹目录”权限所允许的操作 枚举各个文件夹，以便访问其他文件和文件夹，即使该用户没有那些文件夹的权限
修改	包括“写入”权限及“读取及执行”权限所允许的操作 删除文件夹
完全控制	包括其他所有 NTFS 权限允许的操作 更改权限，取得所有权和删除子文件夹和文件

5. 用户享有的权利

用户权利应用目标是授权。权限可以授权对不同对象的不同访问，但是权利却能给予一个用户做特殊事情的能力。用户权利定义了对资源的访问能力。虽然用户权利可以应用于单个的用户，但最好是在“组”基础上管理。这样可以确保作为组成员登录的账户将自动继承该组的相关权利。通过对组而不是对单个用户指派用户权利，可以简化用户管理的任务。当组中的用户都需要相同的用户权利时，可以一次对该组指派用户权利，而不是重复地对每个单独的用户指派相同的用户权利。

如果用户是多个组的成员，则用户权利是累积的，这意味着用户有多组权利。要删除用户的权利，管理员只需简单地从组中删除用户。

某些权利可以覆盖在对象上设置的权限。例如，用户作为备份操作员组的成员登录到域账户时，具有对所有域服务器执行备份操作的权利。但是，这要求能够读取这些服务器上的所有文件，甚至是文件所有者已经明确设置对所有用户（包括备份操作员组成员）都拒绝访问的文件。在这种情况下，执行备份的用户权利优先于所有的文件和目录权限。

9.3.2 用户生命周期

在域中，用户的生命周期主要体现在从规划到消亡的全过程。主要经历以下几个阶段：

- 用户规划，如定义用户名称、定义功能组等。
- 申请用户，如申请用户名称、设置默认密码、在 Active Directory 中的权限、在应用系统的权限、邮件系统的权限等。
- 创建用户，如创建域用户，设置密码等。
- 用户授权，如权限委派、目标、网络访问权限等。
- 用户审核，如识别恶意用户、密码策略、审核等。
- 禁用用户，如禁止用户在 Active Directory 中的权限、在应用系统的权限、邮件系统的权限等。
- 删除用户，如删除在 Active Directory 中的权限、在应用系统的权限、邮件系统的权限等。

1. 用户规划

用户规划主要完成以下功能，如定义组织单位、定义功能组、定义用户名称等。

(1) 定义组织单位。

首先需要定义目标用户所在的组织单位。例如一个企业包括多个子公司，每个子公司在 Active Directory 中以组织单位的方式表示，因此在定义用户时，首先要设置该用户属于哪个组织单位。

(2) 定义功能组。

定义用户所在的功能组，功能组根据需要设置，例如设置财务组、部门组等。以上例为基础，如果每个子公司中包含完整的管理体系，包括相同的财务组、部门组等，在 Active Directory 中要保持命名的唯一性。

(3) 定义用户名称。

在企业网络中，使用计算机的每个人都拥有一个账户，计算机使用者使用他们自己的账户可以使用企业网络中指定的资源，完成与其相对应的任务。

在企业网络中，除了每个人有一个用户外，还可能为此用户对应提供的一些服务如企业电子邮件服务、企业办公自动化的登录账户等。所以，通常情况下，都是使用统一的方式进行命名，一是让计算机的使用者记住自己的用户名，另外，通常用户名还与企业为其提供的电子邮件相对应（如用户名为 wsj，企业电子邮件是 wsj@book.com）。

命名习惯通常如下：

- 对于每个使用者，通常都是使用其“姓”的全称+“名”的简称，例如王淑江的用户名为 wangsjsj。
- 如果使用简称之后有“重名”的现象，可以对重名的用户使用全称或者加序号标识，例如 wangsjsj01。

2. 申请用户

主要完成以下功能，如申请用户名称、设置默认密码、在 Active Directory 中的权限、在应用系统的权限和邮件系统的权限等。

管理员可以做一个统一的模板，描述申请用户时需要设置的内容。例如

申请域用户：	<input type="checkbox"/> 是	<input type="checkbox"/> 否
用户名称：	<input type="checkbox"/> 是	<input type="checkbox"/> 否
登录 Internet：	<input type="checkbox"/> 是	<input type="checkbox"/> 否
电子邮件：	<input type="checkbox"/> 是	<input type="checkbox"/> 否
即时消息系统：	<input type="checkbox"/> 是	<input type="checkbox"/> 否
财务系统：	<input type="checkbox"/> 是	<input type="checkbox"/> 否（根据实际需要设置目标业务系统）

3. 创建用户

主要完成以下功能，如创建域用户。

在 Windows 网络中，如果部署基于 Active Directory 的管理平台，则在“Active Directory 用户和计算机”功能组，提供创建域用户向导，使用该向导即可完成创建用户功能。如果也部署了 Exchange Server2003 邮件系统，在域用户的过程中，将同时创建并启用用户邮件功能。

网管天下 网管经验谈

（1）设置密码。

密码是用户登录网络的钥匙，如果没有钥匙总是要费一番力气后，才能登录到目标操作系统。无论入侵者采用何种远程攻击，如果无法获得管理员或超级管理员的用户密码，就无法完全控制整个系统。若想访问系统，最简单也是必要的方法就是窃取用户的密码。因此，对管理员账户来说，最需要保护的就是密码，如果密码被盗，也就意味着灾难的降临。

据统计，大约 70% 以上的安全隐患是由于密码设置不当引起的。因此，密码的设置无疑是十分讲求技巧的。在设置密码时，请遵守密码安全设置原则，该原则适用于任何使用密码的场合。

① 禁止让账号与密码相同。

如果密码设置与用户账号相同，几乎所有的密码破解软件都将轻而易举的探测出来。

② 禁止使用自己的姓名作为密码。

使用自己的姓或名、甚至是姓名作为密码，实在是不堪一击。对于本单位和熟悉本单位的人来讲，姓名无疑是攻击的首选，因为这几乎谁都能猜得到。

③ 禁止使用常用的英文词组。

一些常用或别致的英文单词往往是用户设置密码时的最爱。在他们看来，这类密码既便于记忆，又凸显自己的个性。但事实上，那些绝顶聪明的入侵者们也早已猜到并详细地将其编入密码猜解字典之中，因此，常用英文词组绝不可用做密码。

④ 禁止使用特定意义的日期。

以具有特定意义的日期作为密码是任何人都十分喜爱。这一类日期通常有自己生日、父母生日、儿女生日、朋友生日、重大节日和个人纪念日等。不用说熟悉的人可以猜得到，即使是陌生人也可以通过穷举的方式而得手。在入侵者的密码猜解字典中，几乎全部罗列以上所有的几个组合。

⑤ 禁止使用简单的密码。

一个以密码暴力猜解软件每秒钟可以尝试 10 万次之多。字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

⑥ 建议经常修改密码。

账户密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改复杂密码，以免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。

⑦ 密码设置需要注意的问题。

综上所述，若欲保证密码的安全，应当遵循以下规则：

- 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符。建议将这些符号排列组合使用，以期达到最好的保密效果。
- 用户密码不要太规则，不要使用用户姓名、生日、电话号码和常用单词作为密码。
- 根据 Windows 系统密码的散列算法原理，密码长度设置应超过 7 位，最好 14 位或者更长。
- 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘中，且包含密码的文件是只读的。
- 密码应定期修改，避免重复使用旧密码，应采用多套密码的命名规则。

- 启用账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁。

在 Windows Server 2008 系统中，如果在“密码策略”中启用了“密码必须符合复杂性要求”设置，则对用户的密码设置有如下要求：

- 不包含全部或部分的用户名。
- 长度至少为 7 个字符。
- 包含以下 4 种类型字符中的 3 种字符。
 - 英文大写字母（从 A 到 Z）
 - 英文小写字母（从 a 到 z）
 - 10 个基本数字（从 0 到 9）
 - 非字母字符（例如，!、\$、#、%）

(2) 创建用户。

在基于 Active Directory 架构的网络中，域用户是最小的管理单位，域用户是最容易管理同时又最难管理，如果赋予域用户的权限过大，将对网络安全带来隐患，如果过小将限制域用户的正常工作。同时域用户的种类不同，管理任务也不同。创建域用户是最简单的任务，需要注意域用户的命名规则和密码规则。以 Windows Server 2008 为例说明如何创建新用户。

第 1 步，以管理员身份登录域控制器，选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，显示如图 9-27 所示的“Active Directory 用户和计算机”窗口。

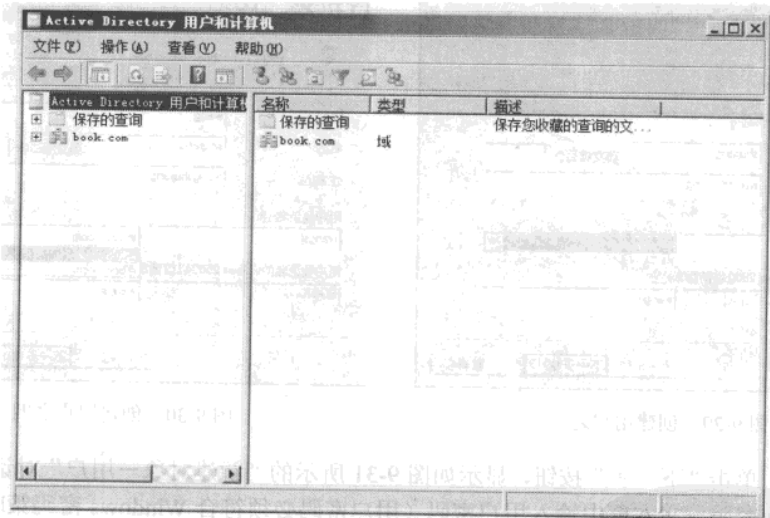


图 9-27 创建用户之一

第 2 步，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，显示如图 9-28 所示的“Active Directory 用户和计算机”窗口。

第 3 步，右击组织单位“Users”，在弹出的快捷菜单中选择“新建”选项，在弹出的级联菜单中选择“用户”命令，显示如图 9-29 所示的“新建对象—用户”对话框。必须要输入“姓名”及“用户登录名”，其他根据需要选择。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

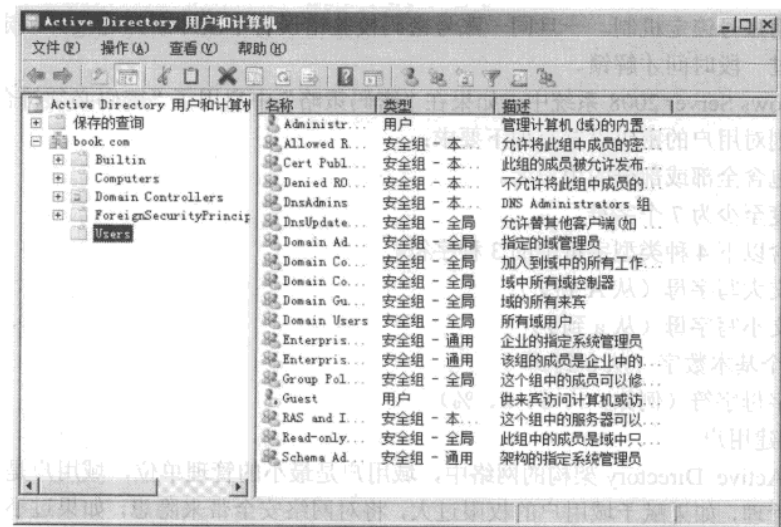


图 9-28 创建用户之二

如果设置了 UPN 后缀，在“用户登录名”右侧的域下拉列表框中，选择 UPN 后缀的名称，如图 9-30 所示。

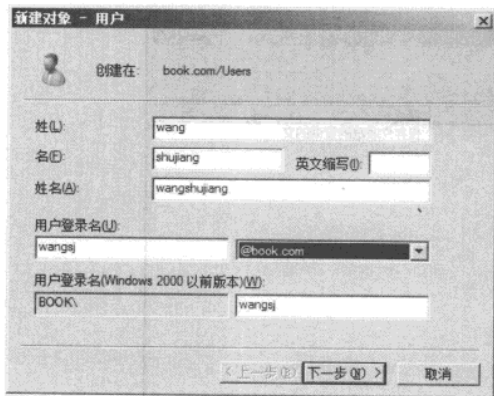


图 9-29 创建用户之三

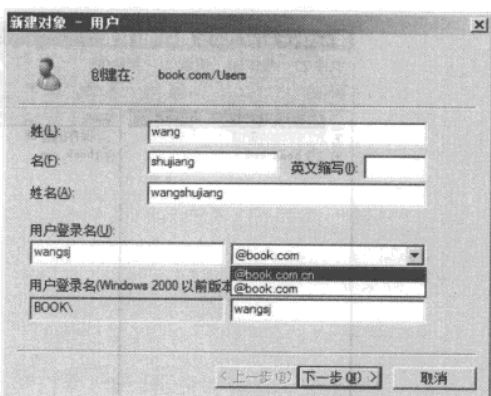


图 9-30 创建用户之四

第 4 步，单击“下一步”按钮，显示如图 9-31 所示的“新建对象—用户”对话框。在“密码”与“确认密码”文本框中输入用户密码（用户密码必须符合 Windows 密码策略），根据需要设置用户的登录属性。

第 5 步，单击“下一步”按钮，显示如图 9-32 所示的“新建对象—用户”对话框。显示新建用户的详细信息。

第 6 步，单击“完成”按钮，创建新的用户。

4. 用户授权

主要完成以下功能，如权限委派、目标组、网络访问权限、登录时间、登录目标等。

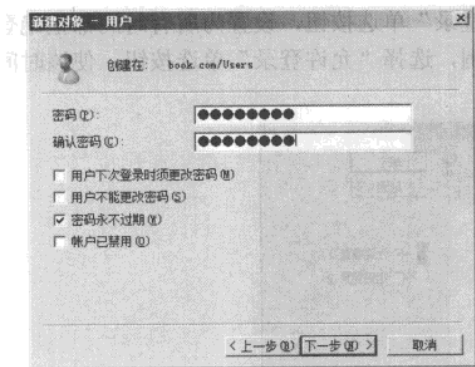


图 9-31 创建用户之五

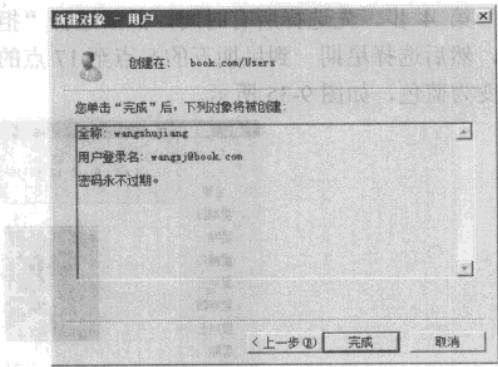


图 9-32 创建用户之六

(1) 登录时间。

默认设置允许网络中的用户在任何时间登录到网络中。在重要的工作环境中，非工作时间不允许用户访问网络中的资源。因此，限制用户在休息时间不能访问网络资源，也是保护网络安全的重要举措，可以有效的防止在工作时间之外的密码破解或者暴力攻击。

在域中，可以限制用户的登录时间，例如限制为只能在某个时间段登录，其他时间不允许登录，从而避免可能在非工作时间产生的恶意攻击。通过以下操作，可以限制用户的登录时间。本例将用户账户“wangsj”限制为每周星期一到星期五的早上 8 点到下午 5 点允许登录。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，显示“Active Directory 用户和计算机”窗口。

第 2 步，在用户列表框中，右击需要重命名的用户，在弹出的快捷菜单中选择“属性”命令，打开“用户属性”对话框，切换到“账户”选项卡，显示如图 9-33 所示的“账户”对话框。

第 3 步，单击“登录时间”按钮，显示如图 9-34 所示“登录时间”对话框，默认允许在任何时间登录。

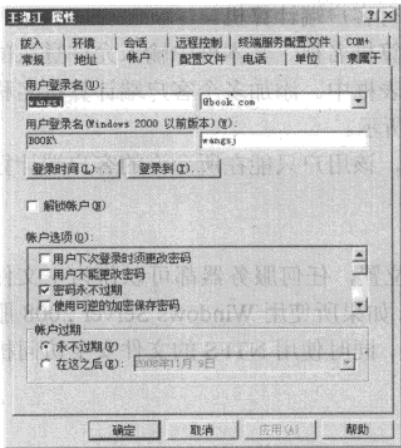


图 9-33 登录目标之一

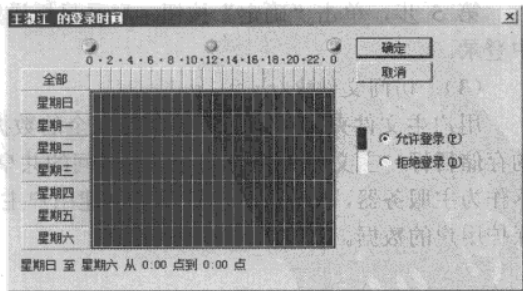


图 9-34 登录时间

网管天下 网管经验谈

第 4 步，先选择所有时间，然后选择“拒绝登录”单选按钮，设置为所有时间都拒绝登录，然后选择星期一到星期五的 8 点至 17 点的范围，选择“允许登录”单选按钮，使该时间段变为蓝色，如图 9-35 所示。

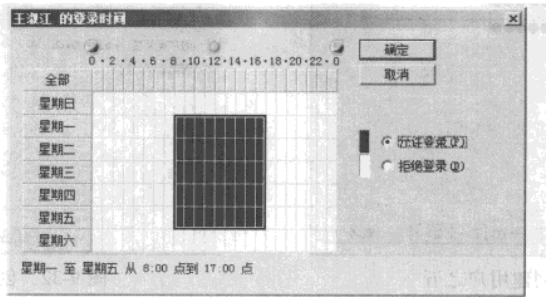


图 9-35 设置登录时间

第 5 步，单击“确定”按钮，用户登录时间设置成功，该用户只能在设定的时间内登录。

(2) 登录目标。

Windows Server 2008 默认设置允许网络中的域用户可以登录到网络中的任何一台计算机，在域中提供限制用户只能在网络中唯一的一台计算机中登录功能，保证用户和计算机逻辑绑定，增强网络安全。通过以下操作，可以在 Active Directory 控制器上限制域用户的登录工作站。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，显示“Active Directory 用户和计算机”窗口。

第 2 步，在用户列表框中，右击需要限制登录的用户，在弹出的快捷菜单中选择“属性”命令，打开“用户属性”对话框，切换到“账户”选项卡，显示如图 9-35 所示的“账户”对话框。

第 3 步，单击“登录到”按钮，显示如图 9-36 所示的“登录工作站”对话框。默认选择“所有计算机”单选按钮，允许用户登录到网络中的所有客户端计算机。

第 4 步，选择“下列计算机”单选按钮，在“计算机名称”文本框中输入允许登录的工作站的 NetBIOS 名称，单击“添加”按钮，添加到列表框中。添加多个客户端计算机名称，将允许该用户在多个指定的工作站上登录，如图 9-37 所示。

第 5 步，单击“确定”按钮，登录目标设置成功，该用户只能在所允许的客户端计算机中登录。

(3) 访问文件夹。

用户主文件夹为域用户提供一个安全的数据存放位置，任何服务器都可以作为主文件夹的存储目标，主文件夹就是允许用户访问的共享空间。如果所使用 Windows Server 2008 服务器作为主服务器，建议在 NTFS 卷上创建用户主文件夹，同时使用 NTFS 的文件安全访问机制保护用户的数据。

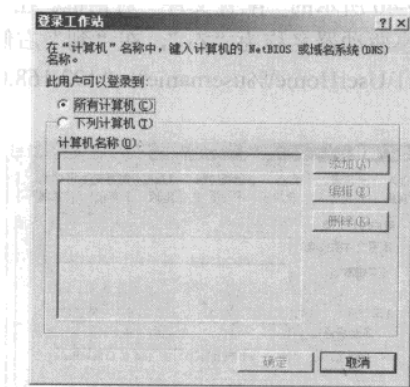


图 9-36 登录目标之二

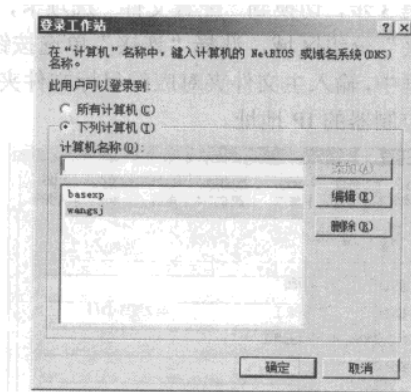


图 9-37 登录目标之三

创建主文件夹包含两方面的内容：

- 创建主文件夹共享文件夹。
- 使用“Active Directory 用户和计算机”指派用户的主文件夹位置。

① 创建共享文件夹。

在运行 Windows Server 2008 服务器上创建共享文件夹“UserHome”，设置共享文件夹的访问权限为“共享”，创建完成的共享文件夹如图 9-38 所示。

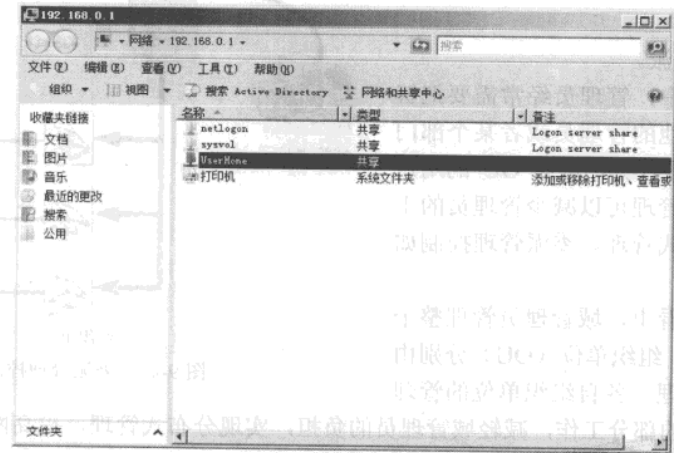


图 9-38 共享文件夹

② 指派用户主文件夹。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，显示“Active Directory 用户和计算机”窗口。

第 2 步，在用户列表框中，右击需要设置主文件夹的用户，在弹出的快捷菜单中选择“属性”命令，显示如图 9-39 所示的“王淑江 属性”对话框。

网管天下 网管经验谈

第3步，切换到“配置文件”选项卡，显示如图9-40所示的“配置文件”对话框。在“主文件夹”分组区域，选择“连接”单选按钮，默认共享驱动器名称为“Z:”，在“到”右侧的文本框中，输入主文件夹对应的目标文件夹\\192.168.0.1\UserHome\%username%， “192.168.0.1”是域控制器的IP地址。

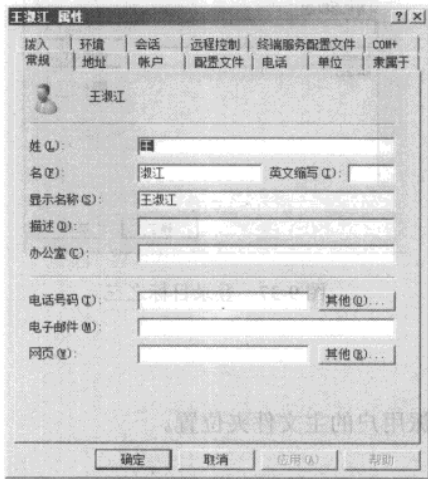


图 9-39 指派用户主文件夹之一

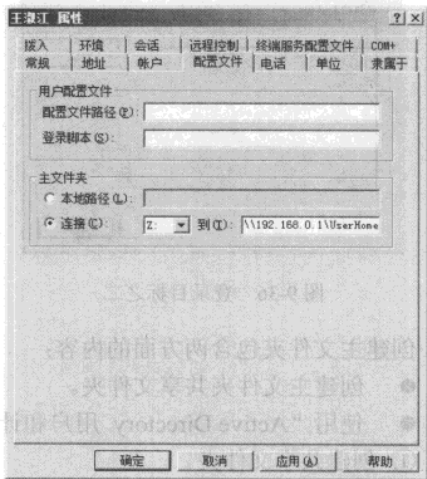


图 9-40 指派用户主文件夹之二

第4步，单击“确定”按钮，用户主文件夹设置成功。

(4) 权限委派。

在网络管理中，管理员经常需要把管理任务委派给其他的管理员或者某个部门的职员来完成管理任务，例如 OU 的用户管理。实施委派管理可以减少管理员的工作量，实现分布式管理。委派管理控制如图9-41所示。

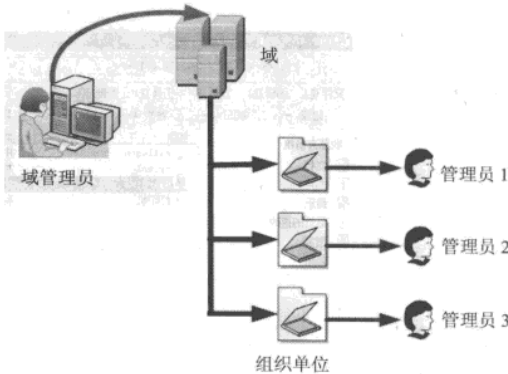


图 9-41 委派管理控制

从图中可以看出，域管理员管理整个 Active Directory，组织单位（OU）分别由各自的管理员管理。各自组织单位的管理员分担域管理员的部分工作，减轻域管理员的负担，实现分布式管理，提高网络的管理效率。

① 委派原则。

在委派用户权限时，建议遵循以下基本原则：

- 范围越大，权限越小。如果要求管理员为企业员工逐一分配系统权限，是件费时费力的工作。系统允许对“组（部门）”进行统一分配，将权限一致的人员编入同一组，然后对该组进行权限分配。
- 权限继承。如果大部门中包含小部门，自动继承大部门的权限。
- 在完成本部门（或角色）工作的前提下，遵循最小授权原则。

② 权限委派。

在 Windows Server 2008 中提供委派向导，根据委派向导即可完成最常用的管理用户任务功能。委派“委派向导”工作的最低层次为组织单位，位于的层次不同，管理的范围也不同，授予的权限也就不同。在使用“委派向导”前，需要管理员仔细规划并详细记录委派任务。

第 1 步，选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开如图 9-42 所示的窗口。

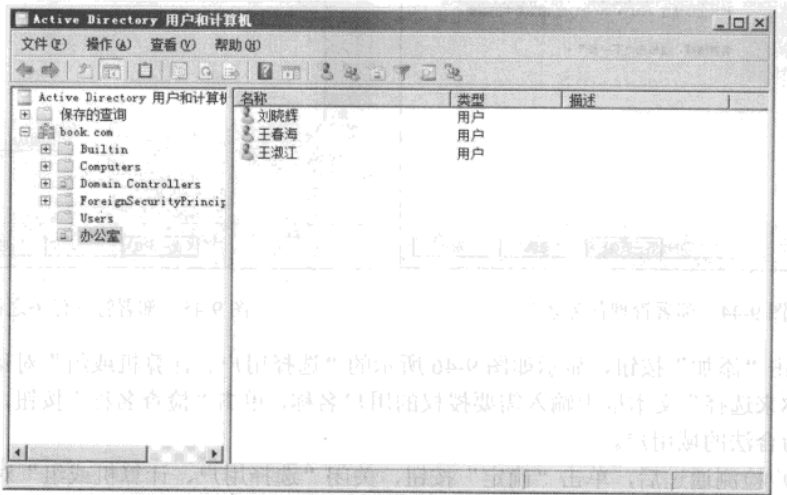


图 9-42 部署管理任务之一

第 2 步，右击目标组织单位，在弹出的快捷菜单中选择“委派控制”命令，如图 9-43 所示。

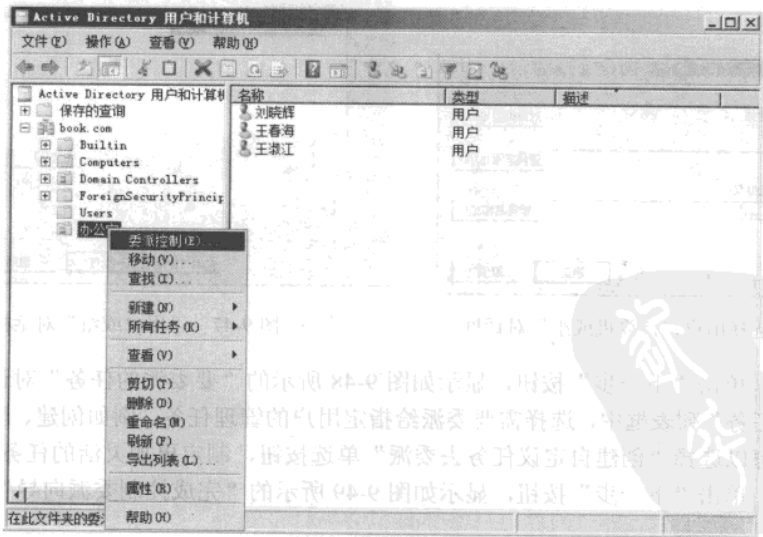


图 9-43 部署管理任务之二

网管天下 网管经验谈

第 3 步，启动“控制委派向导”，显示如图 9-44 所示的“欢迎使用控制委派向导”对话框。

第 4 步，单击“下一步”按钮，显示如图 9-45 所示的“用户或组”对话框。设置委派的目标用户或组。

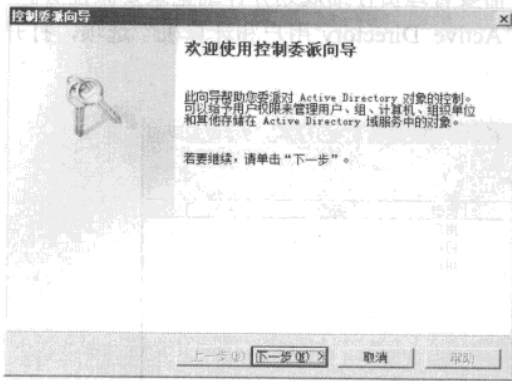


图 9-44 部署管理任务之三

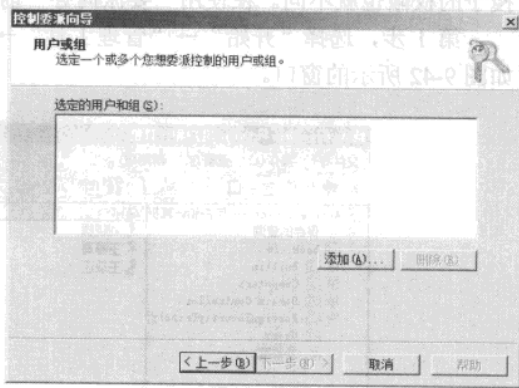


图 9-45 部署管理任务之四

① 单击“添加”按钮，显示如图 9-46 所示的“选择用户、计算机或组”对话框。在“输入对象名称来选择”文本框中输入需要授权的用户名称，单击“检查名称”按钮，检查输入的用户是否为合法的域用户。

② 用户检测通过后，单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“用户或组”对话框，如图 9-47 所示。

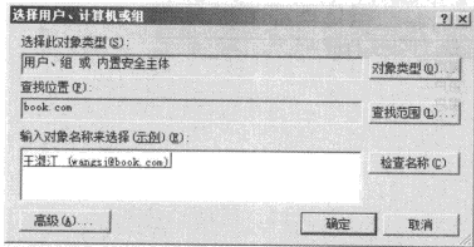


图 9-46 “选择用户、计算机或组”对话框

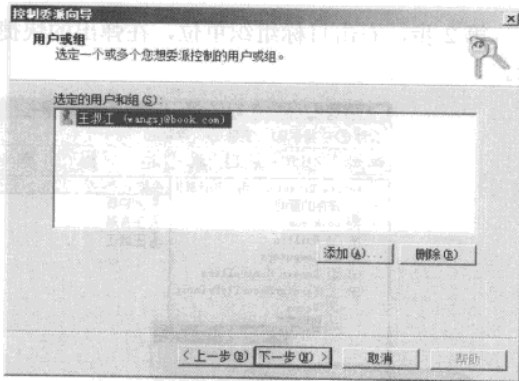


图 9-47 “用户或组”对话框

第 5 步，单击“下一步”按钮，显示如图 9-48 所示的“要委派的任务”对话框。在“委派下列常见任务”列表框中，选择需要委派给指定用户的管理任务，例如创建、删除和管理用户账户。也可以选择“创建自定义任务去委派”单选按钮，制定更加灵活的任务。

第 6 步，单击“下一步”按钮，显示如图 9-49 所示的“完成控制委派向导”对话框。

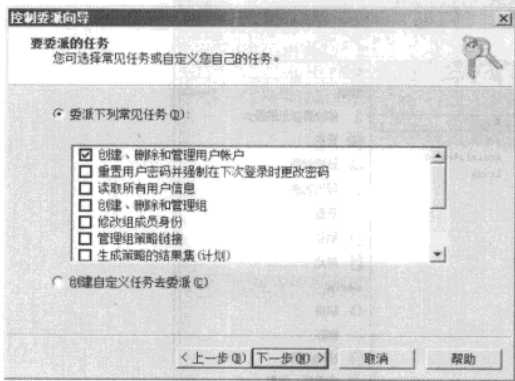


图 9-48 部署管理任务之五

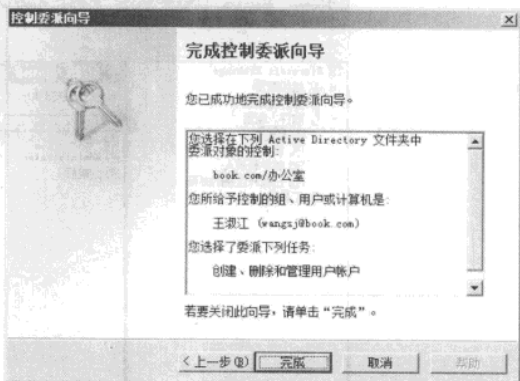


图 9-49 部署管理任务之六

第 7 步，单击“完成”按钮，即可完成用户委派权限的设置。

(5) 用户授权使用电子邮件。

已有用户，是指通过“Active Directory 用户和计算机”管理控制台已经创建的用户。在 Exchange Server 2003 中，如果在域控制器中部署 Exchange 的管理控制台，在创建用户的过程中，可以直接为域用户分配电子邮件地址。在 Exchange Server 2007 SP1 中，将不支持此功能，管理员只能在 Exchange Server 2007 SP1 的管理控制台中，为已经存在的用户分配电子邮件地址。

第 1 步，选择“开始”→“所有程序”→“Microsoft Exchange”→“Exchange 管理控制台”选项，显示如图 9-50 所示的“Exchange 管理控制台”窗口。

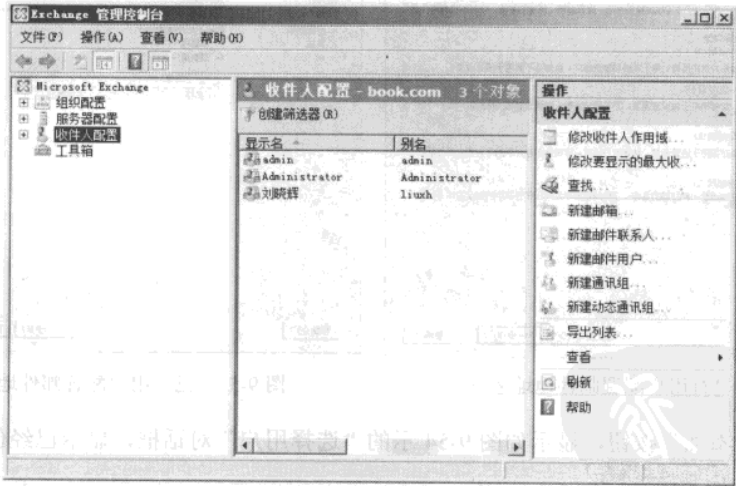


图 9-50 已有用户配置邮件地址之一

第 2 步，选择“Microsoft Exchange”→“收件人配置”→“邮箱”选项，显示如图 9-51 所示的“Exchange 管理控制台”窗口。

网管天下 网管经验谈

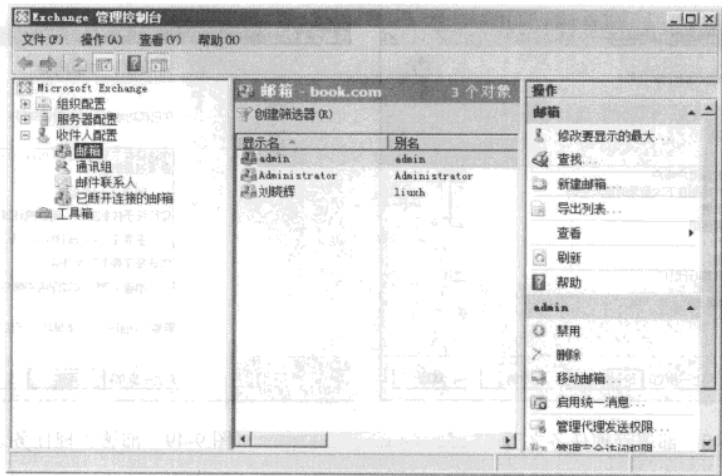


图 9-51 已有用户配置邮件地址之二

第 3 步，在右侧“操作”面板中，单击“新建邮箱地址”超链接，启动“新建邮箱地址”向导，显示如图 9-52 所示的“简介”对话框。介绍该向导允许创建的允许类型，选择“用户邮箱”单选按钮。

第 4 步，单击“下一步”按钮，显示如图 9-53 所示的“用户类型”对话框。选择“现有用户”单选按钮，即使用“Active Directory 用户和计算机”控制台已经创建的用户。

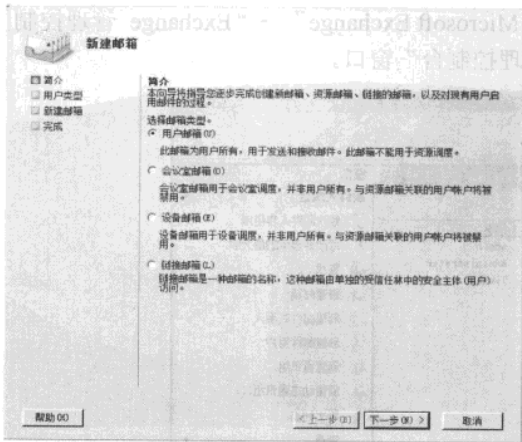


图 9-52 已有用户配置邮件地址之三

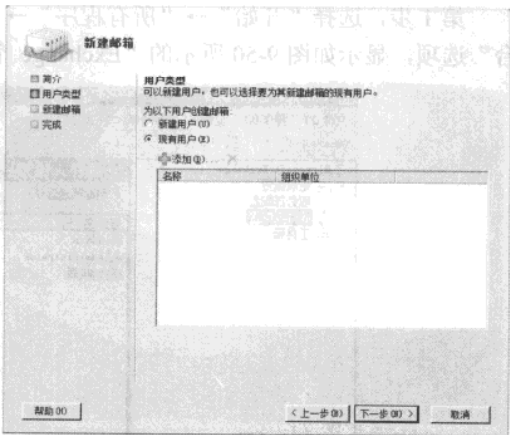


图 9-53 已有用户配置邮件地址之四

- ① 单击“添加”按钮，显示如图 9-54 示的“选择用户”对话框，显示已经创建的用户列表。
- ② 选择需要设置邮箱地址的用户，单击“确定”按钮，关闭“选择用户”对话框，返回到“用户类型”对话框，如图 9-55 所示将选择的用户添加到用户列表中。

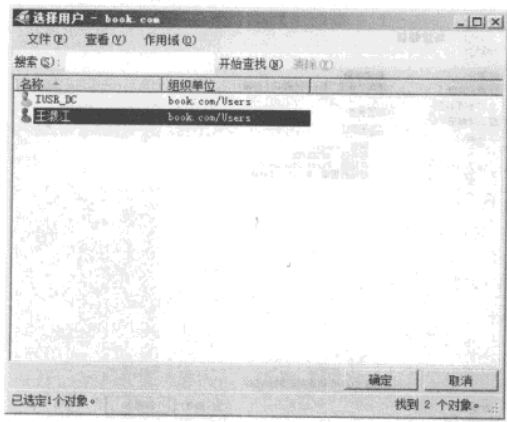


图 9-54 “选择用户”对话框

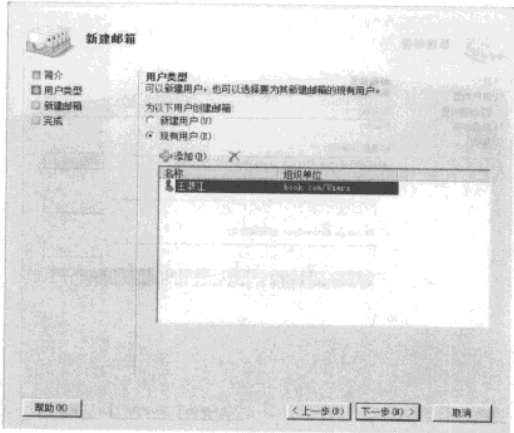


图 9-55 “用户类型”对话框

第 5 步，单击“下一步”按钮，显示如图 9-56 所示的“邮箱设置”对话框，设置选择的用户邮件地址属性。

① 单击“浏览”按钮，显示如图 9-57 所示的“选择邮箱数据库”对话框。显示可用的邮箱数据库列表。如果网络中部署了多个 Exchange 存储组，将在此全部显示。

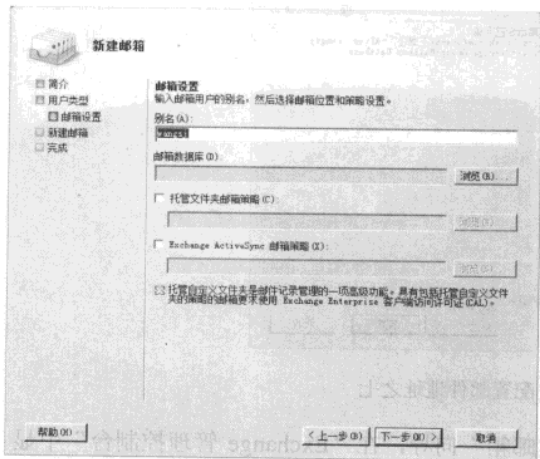


图 9-56 “邮件地址设置”对话框

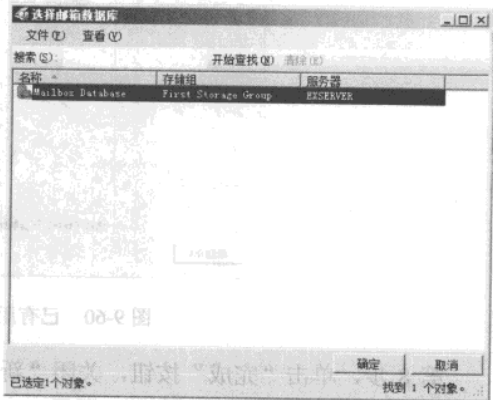


图 9-57 “选择邮件地址数据库”对话框

② 选择目标邮箱数据库，单击“确定”按钮，关闭“选择邮箱数据库”对话框，返回到“邮箱设置”对话框，如图 9-58 所示。

第 6 步，单击“下一步”按钮，显示如图 9-59 所示的“新建邮箱”对话框。

第 7 步，单击“新建”按钮，显示如图 9-60 所示的“完成”对话框，成功创建指定用户的邮件地址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

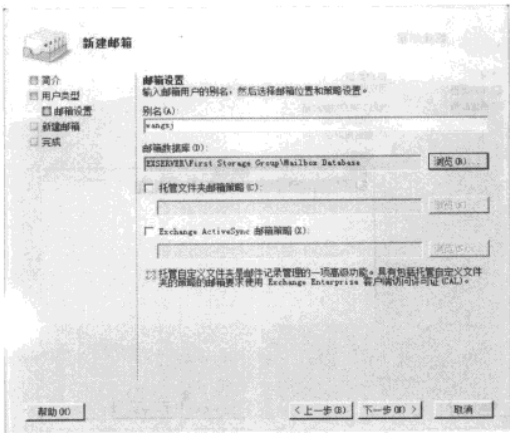


图 9-58 “邮件地址设置”对话框

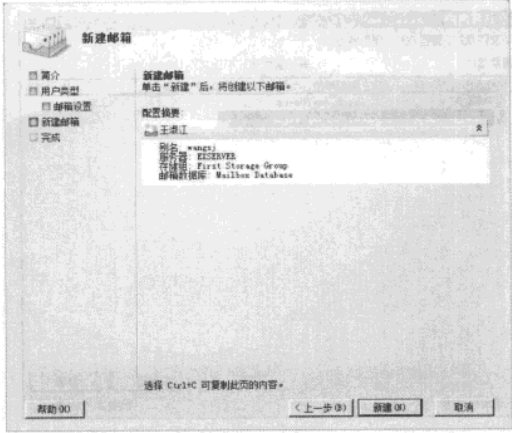


图 9-59 已有用户配置邮件地址之六

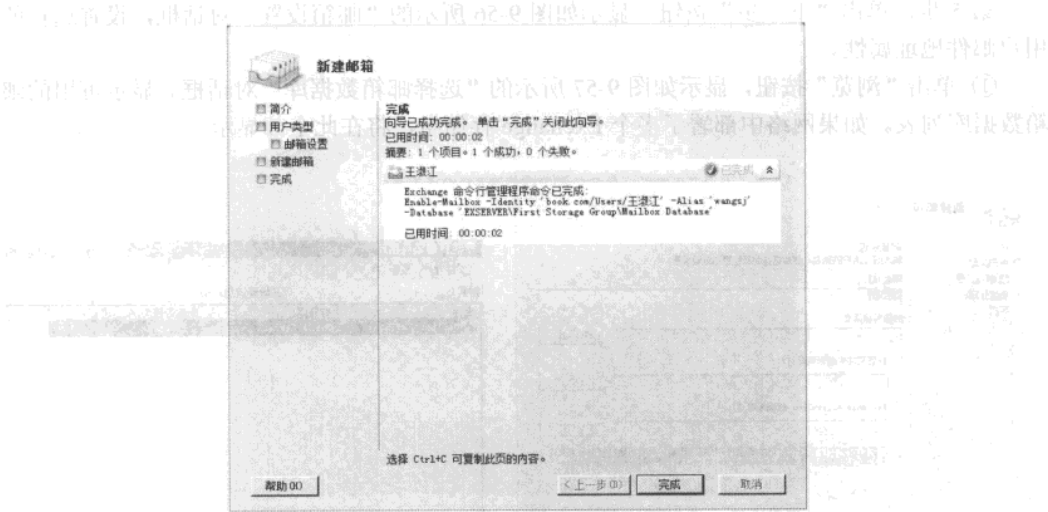


图 9-60 已有用户配置邮件地址之七

第 8 步，单击“完成”按钮，关闭“新建邮箱”向导，在“Exchange 管理控制台”中显示成功创建的邮件地址，如图 9-61 所示。

5. 用户审核

主要完成以下功能，如识别恶意用户、密码策略、审核等。

(1) 密码策略。

密码策略用于保护域或本地用户账户密码安全，设定密码规则等。在 Windows Server 2008 系统中，默认已经为所有用户账户启用了密码策略，包括：

- 密码必须符合复杂性要求。
- 最短密码长度最小值。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

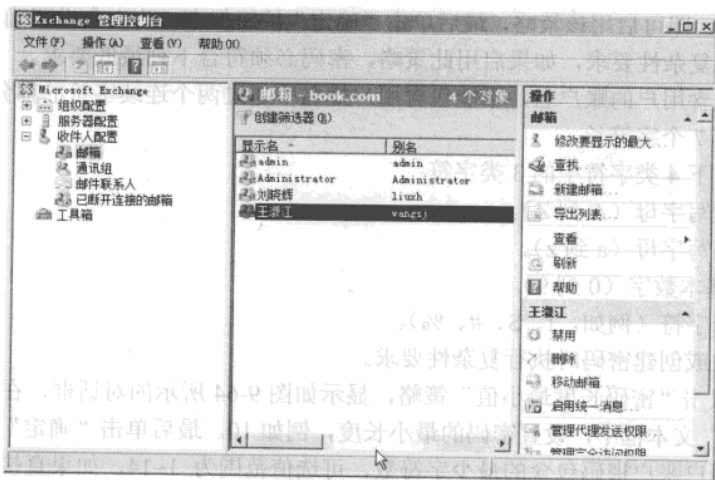


图 9-61 已有用户配置邮件地址之八

- 密码最短使用期限。
- 密码最长使用期限。
- 强制密码历史。
- 用可还原的加密来储存密码。

第 1 步，以管理员身份登录域控制器，选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理编辑器”窗口。选择并编辑“Default Domain Policy”策略，在“组策略管理编辑器”中，选择“密码必须符合复杂性要求”策略，如图 9-62 所示。

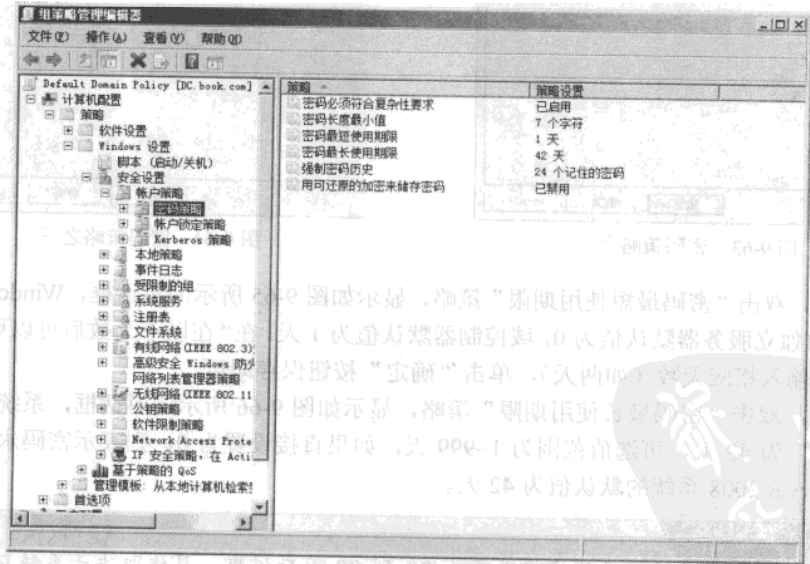


图 9-62 密码策略之一

第 2 步，双击“密码必须符合复杂性要求”策略，显示如图 9-63 所示的对话框，选择“已

网管天下 网管经验谈

启用”单选按钮，即可启用该策略，最后单击“确定”按钮保存。此安全设置确定用户账户密码是否符合复杂性要求，如果启用此策略，密码必须符合下列最低要求。

- 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分
- 至少有 7 个字符长。
- 包含以下 4 类字符中的 3 类字符：
 - 英文大写字母（A 到 Z）。
 - 英文小写字母（a 到 z）。
 - 10 个基本数字（0 到 9）。
 - 非字母字符（例如，!、\$、#、%）。
- 在更改或创建密码时执行复杂性要求。

第 3 步，双击“密码长度最小值”策略，显示如图 9-64 所示的对话框，在“密码必须至少是 xx 个字符”文本框中，设置密码的最小长度，例如 10。最后单击“确定”按钮保存。此安全设置确定用户账户密码包含的最少字符数，可选值范围为 1~14，如果直接设置为 0，则表示允许不设置密码。在 Windows Server 2008 系统中，独立服务器的默认值为 0，而域控制器默认值为 7。

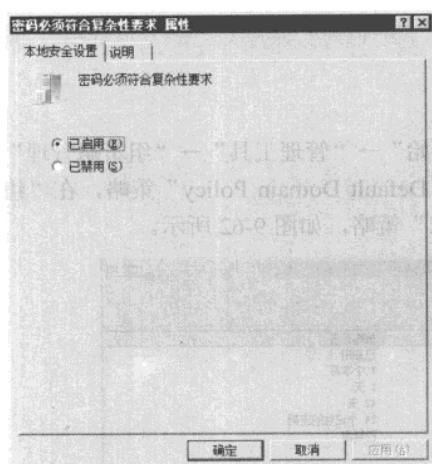


图 9-63 密码策略之二

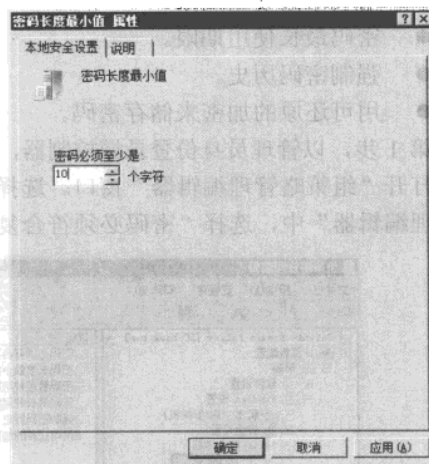


图 9-64 密码策略之三

第 4 步，双击“密码最短使用期限”策略，显示如图 9-65 所示的对话框，Windows Server 2008 系统的独立服务器默认值为 0，域控制器默认值为 1 天。在“在以下天数后可以更改密码”文本框中，输入相应天数（如两天），单击“确定”按钮保存即可。

第 5 步，双击“密码最长使用期限”策略，显示如图 9-66 所示的对话框，系统默认“密码过期时间”为 42 天，可选值范围为 1~999 天，如果直接设置为 0，则表示密码永不过期。Windows Server 2008 系统的默认值为 42 天。

提
示

安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于系统环境及需求。这样，攻击者用来破解用户密码，以及访问网络资源的时间将受到限制。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

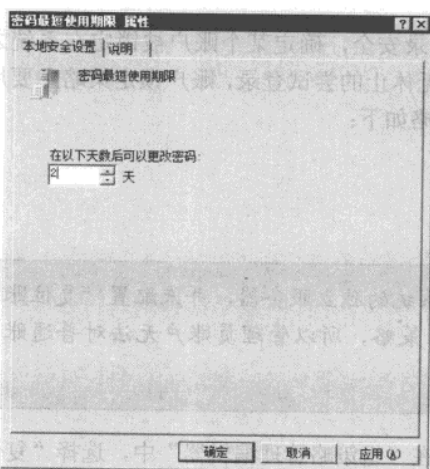


图 9-65 密码策略之四

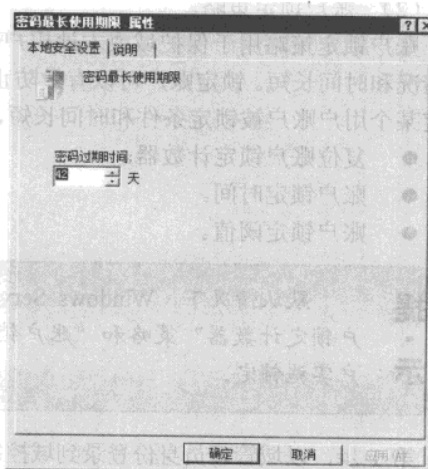


图 9-66 密码策略之五

第 6 步, 双击“强制密码历史”策略, 显示如图 9-67 所示的对话框, 该策略用于限制用户更改账户密码之前不得使用的旧密码个数, 有效范围为 0~24, 例如, 可以设置为 12, 则用户不能重复使用在此之前用过的 12 个历史密码。在 Windows Server 2008 系统中, 独立服务器上默认值为 0, 域控制器上默认值为 24。

第7步，双击“用可还原的加密来储存密码”策略，显示如图9-68所示的对话框，该安全设置确定操作系统是否使用可还原的加密来储存密码。选择“已启用”单选按钮，表示允许使用可还原的加密储存密码，单击“确定”按钮保存设置。使用此安全设置，确定操作系统是否使用可还原的加密来存储密码，此策略还可以为某些应用程序提供支持。使用可还原的加密储存密码与储存纯文本密码，在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。

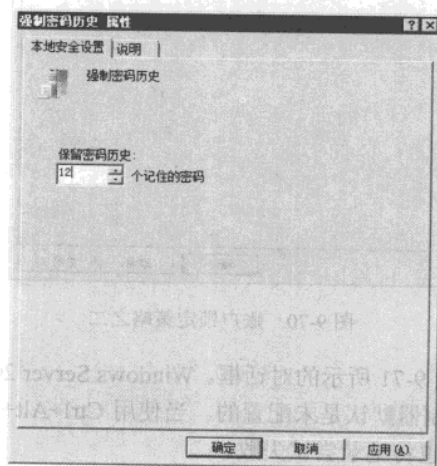


图 9-67 密码策略之六

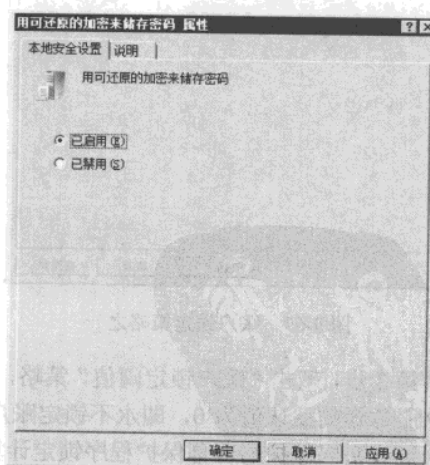


图 9-68 密码策略之七

网管天下 网管经验谈

（2）账户锁定策略。

账户锁定策略用于保护域或本地用户账户的登录安全，确定某个账户被锁定在系统之外的情况和时间长短。锁定账户可以有效防止入侵者无休止的尝试登录，账户锁定策略主要用于确定某个用户账户被锁定条件和时间长短，具体策略如下：

- 复位账户锁定计数器。
- 账户锁定时间。
- 账户锁定阈值。

提示 默认情况下，Windows Server 2008 系统的独立服务器，并未配置“复位账户锁定计数器”策略和“账户锁定时间”策略，所以管理员账户无法对普通账户实施锁定。

第 1 步，以域管理员身份登录到域控制器中，在“组策略管理编辑器”中，选择“复位账户锁定计数器”策略，显示如图 9-69 所示的对话框，选择“定义这个策略设置”复选框，并在“在此后复位账户锁定计数器”文本框中，输入适当的时间值，默认为 30 分钟，即账户被锁定 30 分钟后，方可再次尝试登录。如果定义了账户锁定阈值，此重置时间必须小于或等于账户锁定时间。

第 2 步，双击“账户锁定时间”策略，显示如图 9-70 所示的对话框，选择“定义这个策略设置”复选框，并在“账户锁定时间”文本框中，输入适当的时间值，默认锁定时间为 30 分钟。需要注意的是，只有在指定了账户锁定阈值时，此策略设置才有意义。

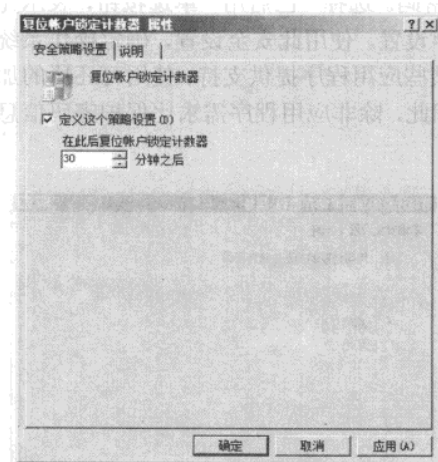


图 9-69 账户锁定策略之一

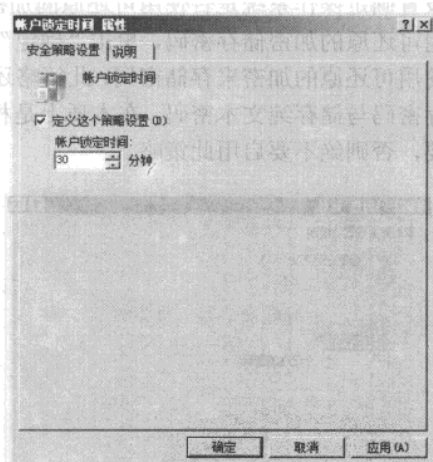


图 9-70 账户锁定策略之二

第 3 步，双击“账户锁定阈值”策略，显示如图 9-71 所示的对话框。Windows Server 2008 独立服务器的默认值为 0，即永不锁定账户，域控制器默认是未配置的。当使用 Ctrl+Alt+Del 组合键或密码保护的屏幕保护程序锁定计算机时，也将记录尝试失败。

网管天下 网管经验谈

Windows Server 2008 系统支持的事件审核策略包括：

- 审核策略更改：确定是否对用户权限分配策略、审核策略或信任策略做出更改的每一个事件进行审核。系统默认设置为“成功”，建议设置为“成功”和“失败”。
- 审核登录事件：确定是否审核用户登录到该计算机、从该计算机注销或建立与该计算机的网络连接的每一个实例。如果设定为审核“成功”，则可用来确定哪个用户成功登录到哪台计算机；如果设定为审核“失败”，则可以用来检测入侵，但攻击者生成的庞大的登录失败日志，会造成拒绝服务（DoS）状态。建议保持系统设置的“成功”状态。
- 审核对象访问：确定是否审核用户访问某个对象，例如，文件、文件夹、注册表项、打印机等，它们都指定了自己的系统访问控制列表（SACL）的事件。建议设置为“失败”。
- 审核进程跟踪：确定是否审核事件的详细跟踪信息，例如，程序激活、进程退出、间接对象访问等。如果怀疑系统被攻击，可启用该项，系统默认设置为“成功”。
- 审核目录服务访问：确定是否审核用户访问那些指定有自己的系统访问控制列表（SACL）的 Active Directory 对象的事件。启用后会在域控制器的安全日志中生成大量审核项，因此只有在确实要使用所创建的信息时才应启用。系统默认设置为“成功”。
- 审核特权使用：此安全设置确定是否审核执行用户权限操作所涉及的实例，但除跳过遍历检查、调试程序、创建标记对象、替换进程级别标记、生成安全审核、备份文件和目录、还原文件和目录等权限。系统默认为“无审核”。
- 审核系统事件：用于确定当用户重新启动或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，是否予以审核。这些事件信息是非常重要的，所以建议设置为“成功”和“失败”。
- 审核账户登录事件：用于确定当用户登录到其他计算机（该计算机用于验证其他计算机中的账户）或从中注销时，是否进行审核。建议设置为“成功”和“失败”。
- 审核账户管理：用于确定是否对计算机上的每个账户管理事件，如重命名、禁用或启用用户账户、创建、修改或删除用户账户和管理事件进行审核。建议设置为“成功”和“失败”。

审核项目应配置得当，如果审核项目过多，不仅会影响服务器的响应速度，而且还会产生大量的日志文件，加重管理员工作负担。如果审核项目不足，则无法准确记录恶意入侵和攻击情况，降低系统安全性。管理员可以在“事件查看器”中“Windows 日志”下的“安全”目录中查看产生的安全性日志。此处以配置“审核策略更改”策略为例，介绍 Windows Server 2008 本地计算机审核策略的配置。

第 1 步，在“审核策略”窗口中，双击“审核策略更改”策略，显示如图 9-73 所示的“审核策略更改 属性”对话框。同时选中“成功”和“失败”复选框，即可同时记录所有“成功”和“失败”的策略更改事件。在域控制器上该策略默认为只审核“成功”的操作，在独立服务器上默认设置为“无审核”，即不记录任何此类事件。

第 2 步，切换到如图 9-74 所示的“说明”选项卡，可以查看该策略的说明信息。

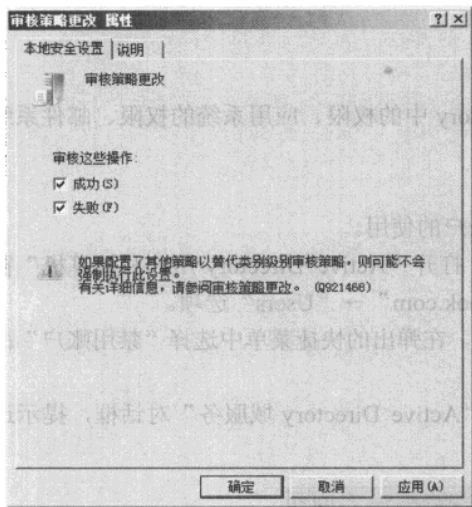


图 9-73 配置审核之二

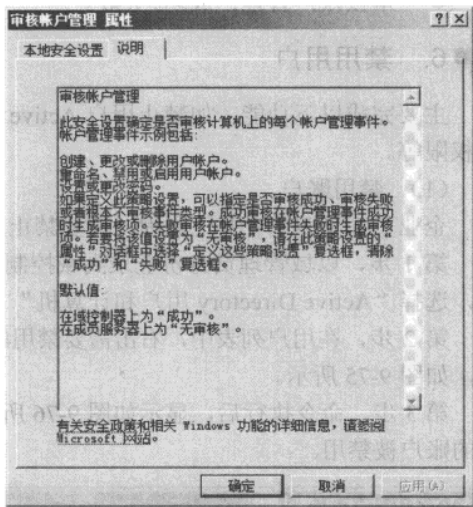


图 9-74 配置审核之三

第 3 步，单击“确定”按钮，保存设置即可。配置其他审核策略的操作步骤与之完全相同，此处不复赘述。

(4) 推荐的策略设置。

推荐的密码策略配置目标为：

- “密码必须符合复杂性要求”——已启用，必须启用。
- “密码长度最小值”——8 个字符或者更高。

推荐的账户锁定策略为：

- “账户锁定阈值”——3 次（或者略高）无效登录。
- “账户锁定时间”——30 分钟（默认，可根据实际需要更改）。
- “复位账户锁定计数器”——30 分钟（默认，可根据实际需要更改）之后。

提示

密码复杂性是指密码中必须包含字母、数字、特殊符号等内容。对安全性要求比较高的地方，推荐使用超过 12 位以上的密码长度。密码应该经常性更换，特别在有管理员以外的人知道时。系统管理员 Administrator 密码建议仅有管理员知道，有足够强壮的密码，并且修改默认的用户名。

推荐的审核策略配置目标为：

- 审核策略更改：成功+失败。
- 审核登录事件：成功+失败。
- 审核访问对象：失败。
- 审核目录服务访问：失败。
- 审核特权使用：失败。
- 审核系统事件：成功+失败。
- 审核账户登录事件：成功+失败。

网管天下 网管经验谈

- 审核账户管理：成功+失败。

6. 禁用用户

主要完成以下功能，如禁止用户 Active Directory 中的权限、应用系统的权限、邮件系统的权限等。

(1) 禁用账户。

企业员工离职或者其他原因，需要禁止用户账户的使用。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项。

第 2 步，在用户列表中，右击需要禁用的用户，在弹出的快捷菜单中选择“禁用账户”命令，如图 9-75 所示。

第 3 步，命令执行后，显示如图 9-76 所示的“Active Directory 域服务”对话框，提示选择的账户被禁用。

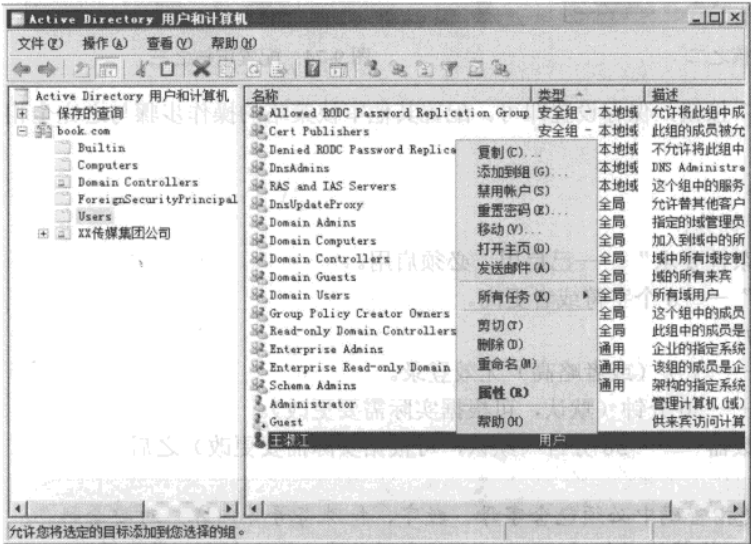


图 9-75 禁用账户之一

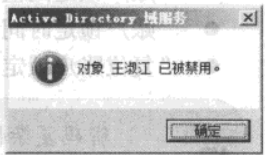


图 9-76 禁用账户之二

第 4 步，单击“确定”按钮，返回到“Active Directory 用户和计算机”窗口。被禁用的账户左侧的图标显示向下的箭头，说明该账户已经被禁用，如图 9-77 所示。

(2) 启用账户。

被禁用的账户并没有从 Windows 活动目录中删除掉，可以根据需要重新启用禁用的账户。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项。

第 2 步，在用户列表中，右击需要启用的用户，在弹出的快捷菜单中选择“启用账户”命令，如图 9-78 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

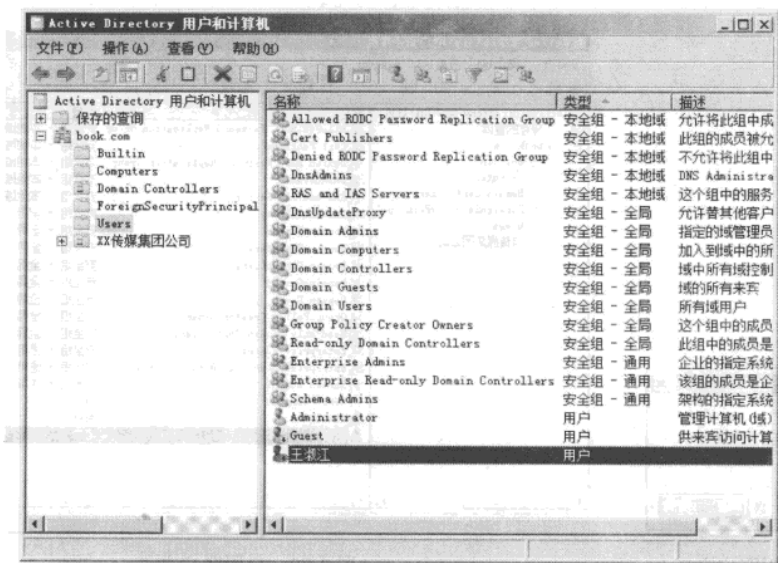


图 9-77 禁用账户之三

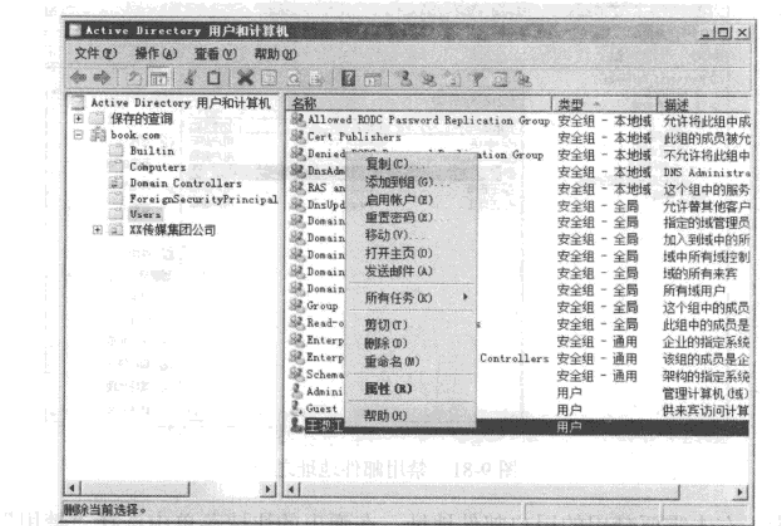


图 9-78 启用账户之一

第 3 步，命令执行后，显示如图 9-79 所示的“Active Directory 域服务”对话框，提示选择的账户被重新启用。

第 4 步，单击“确定”按钮，账户启用成功，如图 9-80 所示。

(3) 禁用邮件。

当用户不需要使用邮件服务后，即可禁止该用户的电子邮件功能。注意，仅禁止用户的邮件功能，不禁止用户登录 Active Directory 的权限。

第 1 步，打开“Exchange 管理控制台”窗口，选择“Microsoft Exchange”→“收件人配置”→“邮箱”选项，显示可用的用户电子邮件列表，如图 9-81 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

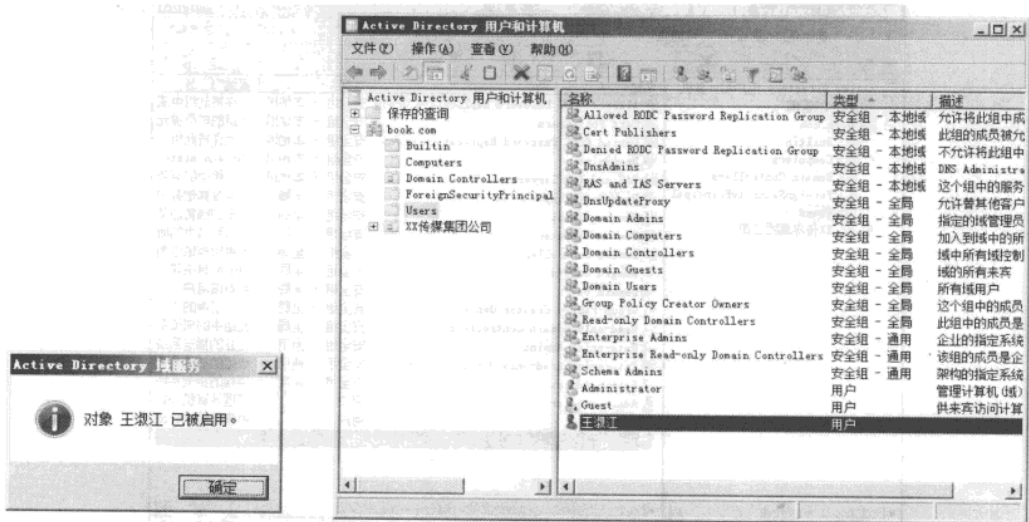


图 9-79 启用账户之二

图 9-80 启用账户之三

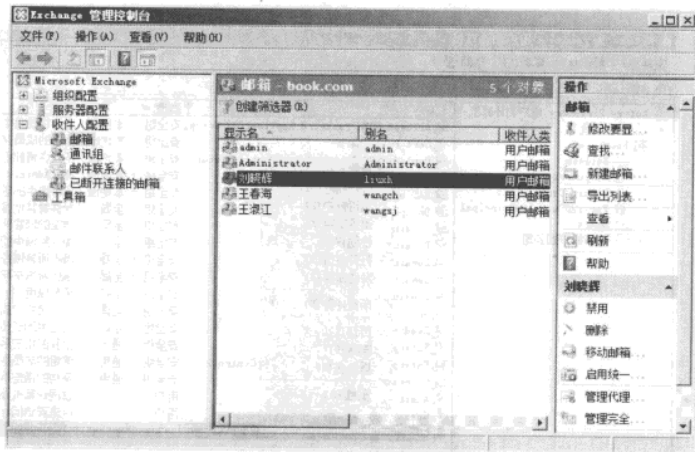


图 9-81 禁用邮件地址之一

第 2 步，右击需要禁用的用户邮件地址，在弹出的快捷菜单中选择“禁用”命令，显示如图 9-82 所示的用户属性对话框。

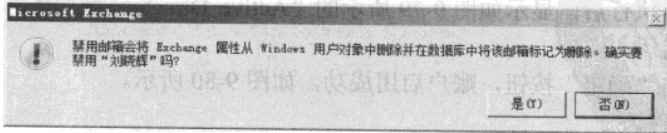


图 9-82 禁用邮件地址之二

第 3 步，单击“是”按钮，禁用选择的用户。用户的电子邮件被禁用后，邮箱列表中将不显示被禁用的电子邮件，如图 9-83 所示。

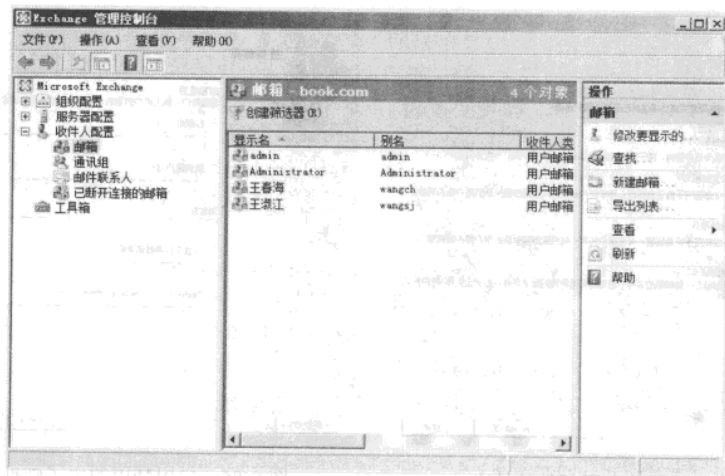


图 9-83 禁用邮件地址之三

第 4 步，被禁用的电子邮件被移动到“已断开连接的邮箱”，如图 9-84 所示。

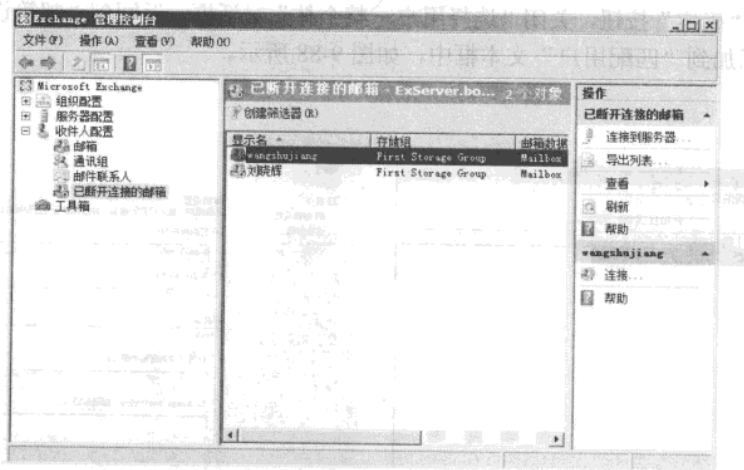


图 9-84 禁用邮件地址之四

(4) 启用禁用的用户邮件。

重新启用被禁用的电子邮件地址。

第 1 步，打开“Exchange 管理控制台”窗口，选择“Microsoft Exchange”→“收件人配置”→“已断开连接的邮箱”选项，显示被禁用的用户电子邮件列表。右击选择需要启用的电子邮件地址，在弹出的快捷菜单中选择“连接”命令，启动“连接邮箱”向导，显示如图 9-85 所示的“简介”对话框。

第 2 步，选择“用户邮箱”单选按钮，单击“下一步”按钮，显示如图 9-86 所示的“邮箱设置”对话框。

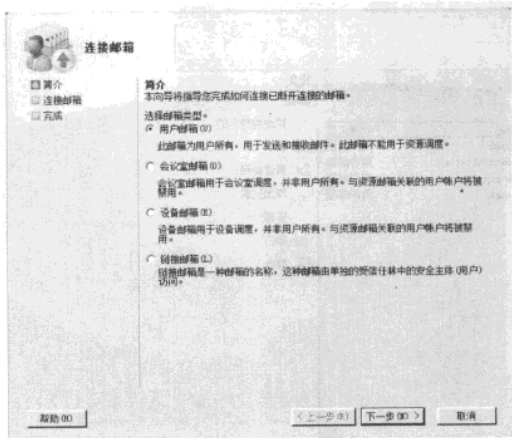


图 9-85 启用禁用的电子邮件地址之一

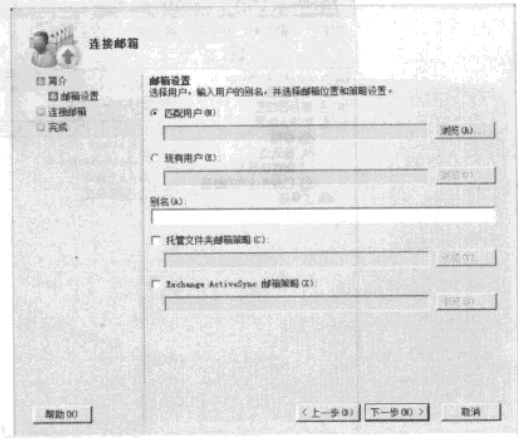


图 9-86 启用禁用的电子邮件地址之二

- ① 单击“浏览”按钮，显示如图 9-87 所示的“选择用户—整个林”对话框。从林中检索被禁用的用户同名的 Active Directory 域用户。
- ② 单击“确定”按钮，关闭“选择用户—整个林”对话框，返回到“邮箱设置”对话框，选择的用户添加到“匹配用户”文本框中，如图 9-88 所示。

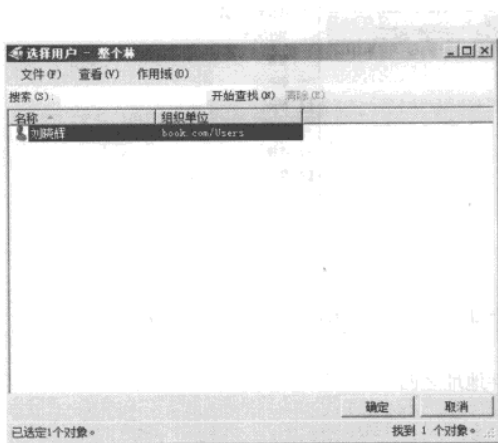


图 9-87 “选择用户—整个林”对话框

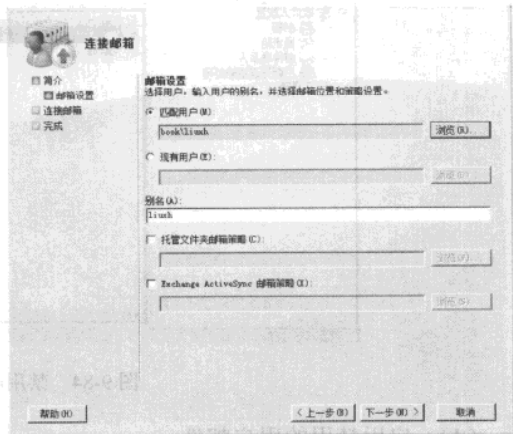


图 9-88 “邮箱设置”对话框

- 第 3 步，单击“下一步”按钮，显示如图 9-89 所示的“连接邮箱”对话框。
- 第 4 步，单击“连接”按钮，恢复被禁用的电子邮件地址，显示如图 9-90 所示的“完成”对话框。
- 第 5 步，用户电子邮件地址恢复成功后，电子邮件地址移动到“收件人配置”→“邮箱”列表框中，如图 9-91 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

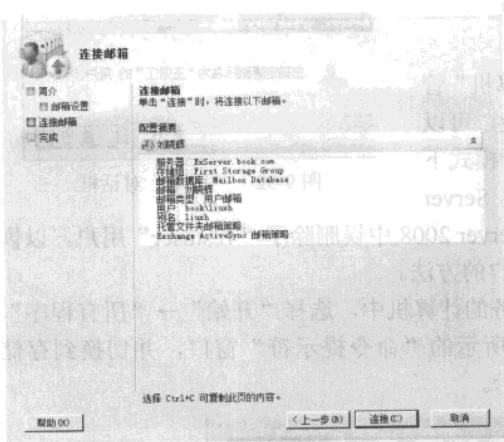


图 9-89 启用禁用的电子邮件地址之三

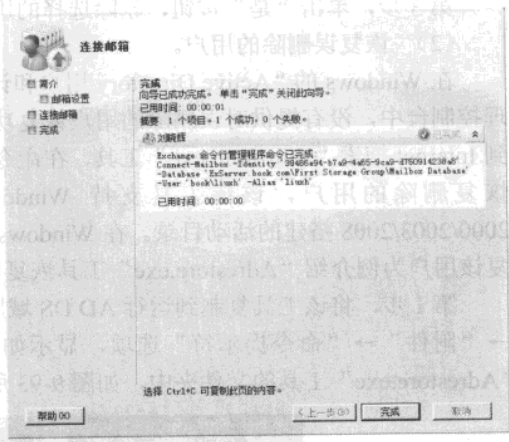


图 9-90 启用禁用的电子邮件地址之四

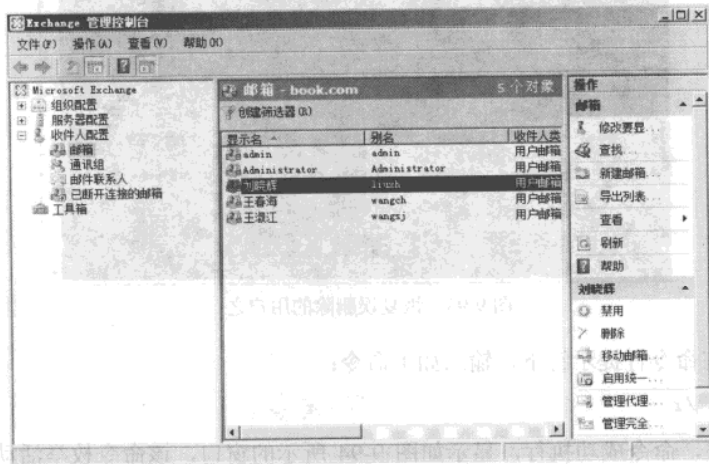


图 9-91 启用禁用的电子邮件地址之五

7. 删除用户

主要完成以下功能，如删除用户在 Active Directory 中的权限、应用系统的权限、邮件系统的权限等。

(1) 删除用户。

员工离职，将此员工从 Active Directory 数据库中彻底删除。建议员工刚离职时，选择账户禁用功能，一段时间之后删除被禁用的账户。

第 1 步，以域管理员身份登录到域控制器中，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项。

第 2 步，在用户列表框中，右击需要删除的用户，在弹出的快捷菜单中选择“删除”命令，显示如图 9-92 所示的“删除”对话框。

网管天下 网管经验谈

第3步，单击“是”按钮，删除选择的用户。
(2) 恢复误删除的用户。

在 Windows 的“Active Directory 用户和计算机”管理控制台中，没有提供对误删除的用户恢复功能，可以到 Internet 搜索“Adrestore.exe”工具，在命令行模式下恢复删除的用户，该工具支持 Windows Server 2000/2003/2008 搭建的活动目录。在 Windows Server 2008 中误删除了“Testuser”用户，以恢复该用户为例介绍“Adrestore.exe”工具恢复用户的方法。

第1步，将该工具复制到运行 AD DS 域服务的计算机中，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，显示如图所示的“命令提示符”窗口，并切换到存储“Adrestore.exe”工具的文件夹中，如图 9-93 所示。

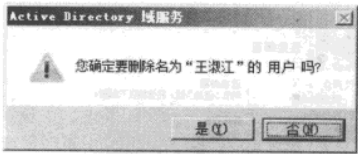


图 9-92 “删除”对话框



图 9-93 恢复误删除的用户之一

第2步，在命令行提示符下，输入如下命令：

```
Adrestore /r
```

按 Enter 键，命令成功执行，显示如图 9-94 所示的窗口，该命令枚举活动目录中删除的对象，并显示用户完整的 FQDN 信息。



图 9-94 恢复误删除的用户之二

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用户、计算机账户管理 | 9

第 3 步，输入“Y”，恢复删除的用户信息，提示用户被成功恢复，如图 9-95 所示。同样的方法可以恢复其他被删除的 Active Directory 对象。

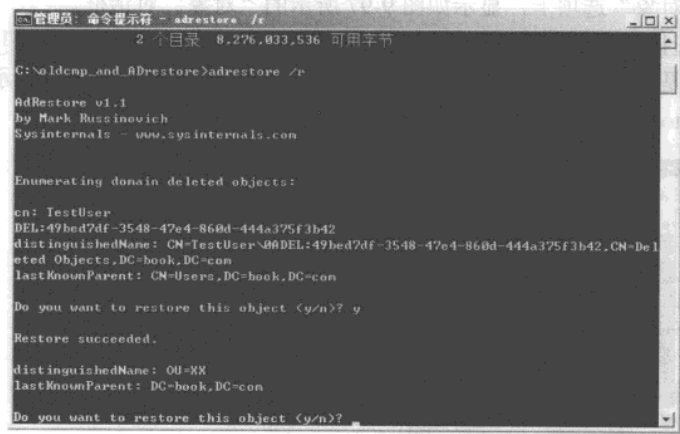


图 9-95 恢复误删除的用户之三

第 4 步，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→“book.com”→“Users”选项，Testuser 被成功恢复，恢复的用户状态为“禁用”，如图 9-96 所示。

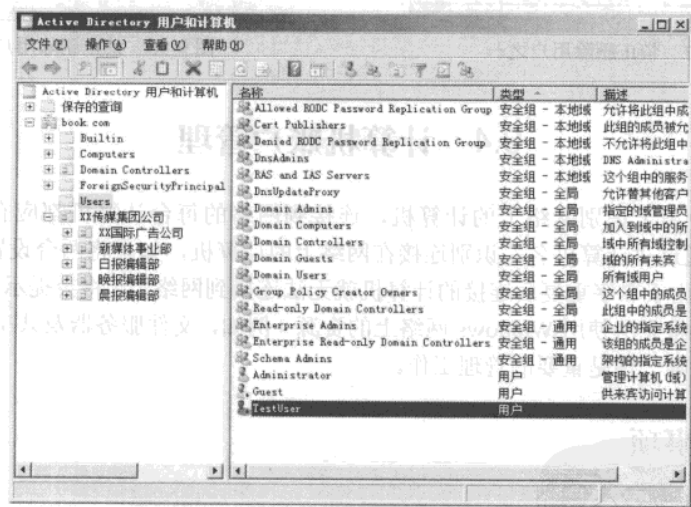


图 9-96 恢复误删除的用户之四

第 5 步，恢复的账户需要重新设置密码，启用该账户即可完整恢复被删除的用户账户。
(2) 禁止删除用户。

Windows Server 2008 的 AD DS 域服务支持禁止删除用户功能，如果执行删除操作将不能删除用户，在用户创建过程中不能设置该功能，只能在创建用户完成后在属性中设置。

第 1 步，打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计

网管天下 网管经验谈

算机”→“book.com”→“Users”选项。

第 2 步，在用户列表中，右击需要禁止删除的用户，在弹出的快捷菜单中选择“属性”命令，切换到“对象”选项卡，显示如图 9-97 所示的“对象”对话框。

第 3 步，选择“防止对象被意外删除”复选框，单击“确定”按钮，即可设置该用户被禁止删除，即使是网络管理员也不可能删除该用户，执行删除功能后，将显示如图 9-98 所示的“Active Directory 域服务”对话框。

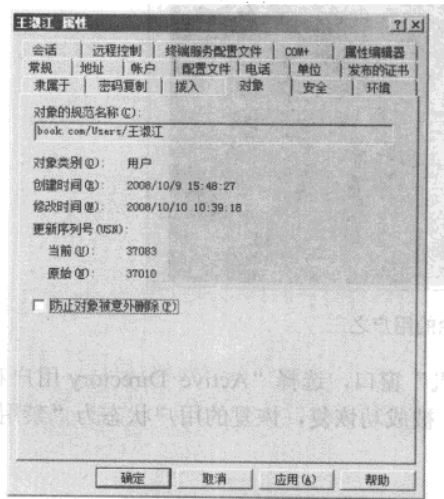


图 9-97 禁止删除用户之一

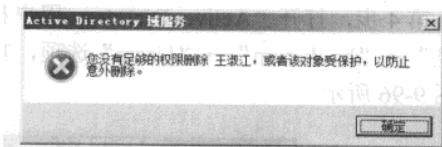


图 9-98 禁止删除用户之二

9.4 计算机账户管理

计算机账户用于识别网络上的计算机，连接到网络的每台计算机都应有唯一的名称。Windows 网络通过“计算机名”识别连接在网络上的计算机，如果将两台设置相同的计算机连接在网络上，由于名字重复后连接的计算机就无法连接到网络上，将会提示“用户名重复”，被拒绝的计算机将无法使用 Windows 网络上的资源（例如，文件服务器及共享打印机），因此保证计算机名的唯一性是重要的管理工作。

9.4.1 注意事项

1. 计算机名命名原则

网络中计算机名表示一台计算机在网络中的身份。一台计算机在网络中只能存在一个计算机账户，合理的规划计算机名对网络管理十分重要。

规划计算机名时，建议遵循以下原则：

- 计算机名的长度不要超过 128 个字符，不能含有空格或下述的任意专用字符：; : " < > * + = \ | ?。

- 如果计算机是专属于一个人使用，则以此人名字完整拼音字母命名计算机。例如，计算机是王淑江使用，则命名为 Wangshujiang。
- 如果一台计算机是多人使用，则以部门名称命名。例如，财务部只有一台计算机，有 10 人使用，则该计算机命名为 Caiwubu。
- 如果一个部门中有多台计算机，命名时以部门简写开始同时添加计算机使用者。例如财务部中的用户王淑江使用的计算机，则命名为 CWB-wangshujiang。
- 计算机命名时，建议不要使用中文，Windows 系统支持中文计算机名。
- 重命名计算机名时，如果计算机名超过 15 个字符，Netbios 名称将自动截断并保存前 15 个字符。
- 如果计算机名称超过 15 个字符，例如 CWB-wangshujiang，建议用户名称以简写或者统一方式命名，例如 CWB-Wangsj。
- 遵循上述原则后仍然出现计算机名重复，建议在计算机名后添加序号标识，例如 CWB-Wangsj01。

2. 计算机账户密码

计算机账户使用的密码不再称之为“密码”，在 Active Directory 中称为“登录票据”，由域控制器上的 KDC 服务颁发与维护。为了保证系统安全，KDC 服务每 30 天自动更新计算机使用的票据，并把上次使用的票据记录下来。也就是说服务器始终保存着两个票据，其有效时间是 60 天，60 天后上次使用的票据被系统丢弃。如果仍然使用上次的票据登录，将提示“账户丢失”。

3. 加域权限

网络中部署 Active Directory 后，普通域用户不具备将客户端计算机加入到 Active Directory 中的权限。在实际的网络管理中，如果客户端计算机数量较少且相对比较集中，管理员可以以手动的方式将客户端计算机加入到 Active Directory 中；如果比较分散且数量较多，建议域用户具备将计算机加入到域中的权限，从而允许用户在计算机安装完成后，将自身加入到 Active Directory 中。

(1) 授予“将工作站添加到域”的权限。

Active Directory 部署完成后，默认只有“Administrators”组的用户具备将计算机加入域的权限，管理员可以授予目标用户具备将计算机加入域的权限。该策略允许添加的计算机账户数量为 10，注意该数字是添加的脚手架，不是添加次数。

第 1 步，以域管理员身份登录到域控制器中，启动组策略管理控制台，选择“Default Domain Policy”策略，启动“组策略管理编辑器”，选择“Default Domain Policy”→“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”选项，显示如图 9-99 所示的“组策略编辑管理器”窗口。

第 2 步，右击“将工作站添加到域”策略，在弹出的快捷菜单中选择“属性”命令，显示如图 9-100 所示的“将工作站添加到域 属性”对话框。

第 3 步，选择“定义这些策略设置”复选框，如图 9-101 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

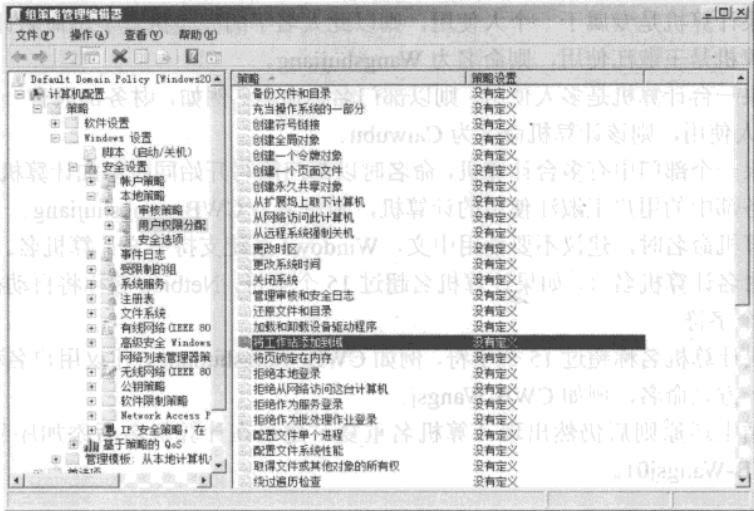


图 9-99 “组策略编辑管理器”窗口

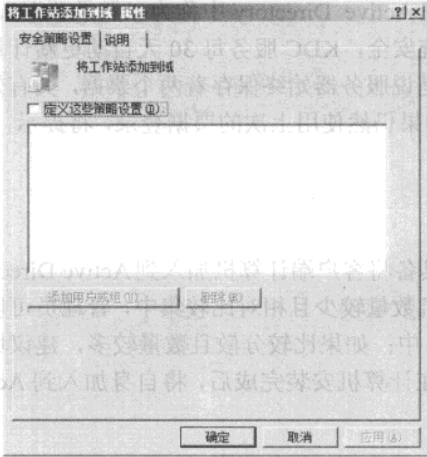


图 9-100 “将工作站加入到域 属性”对话框

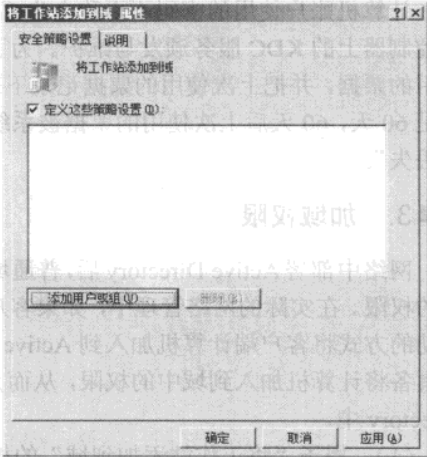


图 9-101 “将工作站加入到域 属性”对话框

- ① 单击“添加用户或组”按钮，显示如图 9-102 所示的“添加用户或组”对话框。
- ② 单击“浏览”按钮，显示如图 9-103 所示的“选择用户、计算机或组”对话框。

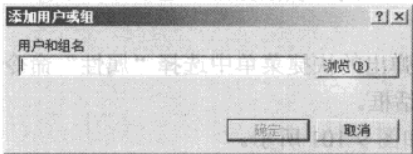


图 9-102 “添加用户或组”对话框

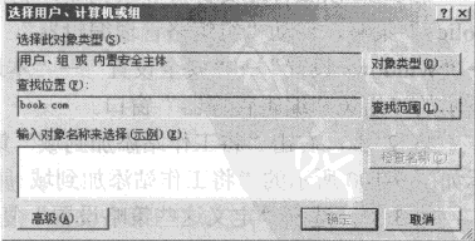


图 9-103 “选择用户、计算机或组”对话框

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用户、计算机账户管理 9

- ③ 单击“高级”按钮，显示如图 9-104 所示的“选择用户、计算机或组”高级对话框。
- ④ 单击“立即查找”按钮，在“搜索结果”列表框中，显示当前域中所有可用的账户或组，如图 9-105 所示。

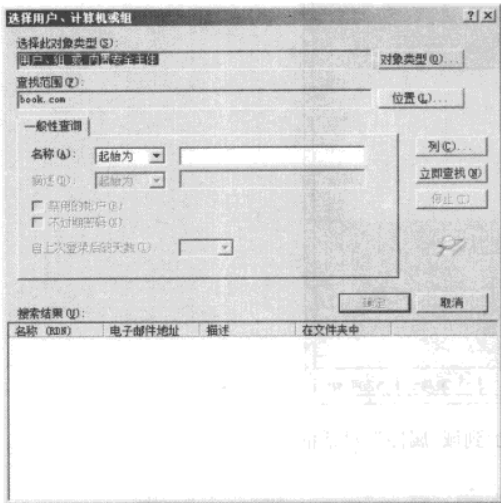


图 9-104 “选择用户、计算机或组”高级对话框

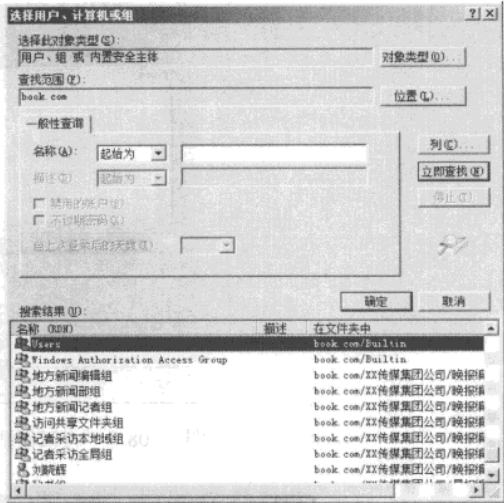


图 9-105 “选择用户、计算机或组”高级对话框

- ⑤ 选择目标组，单击“确定”按钮，关闭“选择用户、计算机或组”高级对话框，返回到“选择用户、计算机或组”对话框，如图 9-106 所示。
- ⑥ 单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“添加用户或组”对话框，如图 9-107 所示。

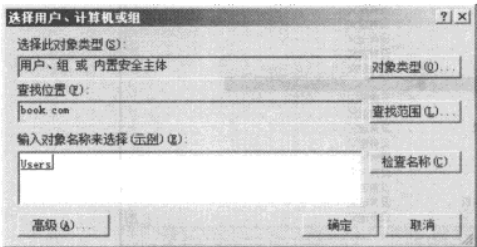


图 9-106 “选择用户、计算机或组”对话框

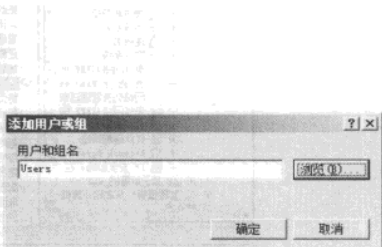


图 9-107 “添加用户或组”对话框

- ⑦ 单击“确定”按钮，关闭“添加用户或组”对话框，返回到“将工作站添加到域 属性”对话框，如图 9-108 所示。
- 第 4 步，单击“确定”按钮，完成策略的设置，如图 9-109 所示。

4. 计算机账户升/降域

Windows 2000 以上操作系统的计算机加入域，不需要提前创建计算机账号，在加入 Active Directory 的过程中自动创建计算机账户，并启用该计算机账户。降域后，计算机账户不能自动从 Active Directory 中删除，禁止该账户的使用。因此升域过程，也是加入 Active Directory

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网管天下 网管经验谈

的过程。

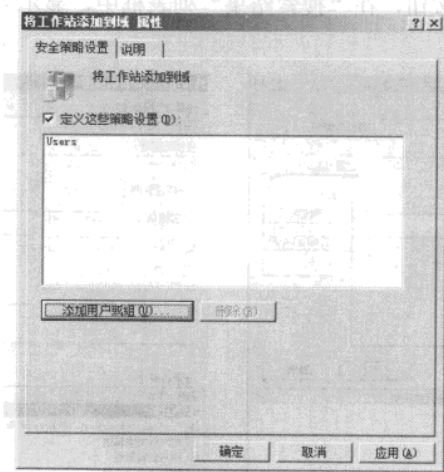


图 9-108 “将工作站添加到域 属性”对话框

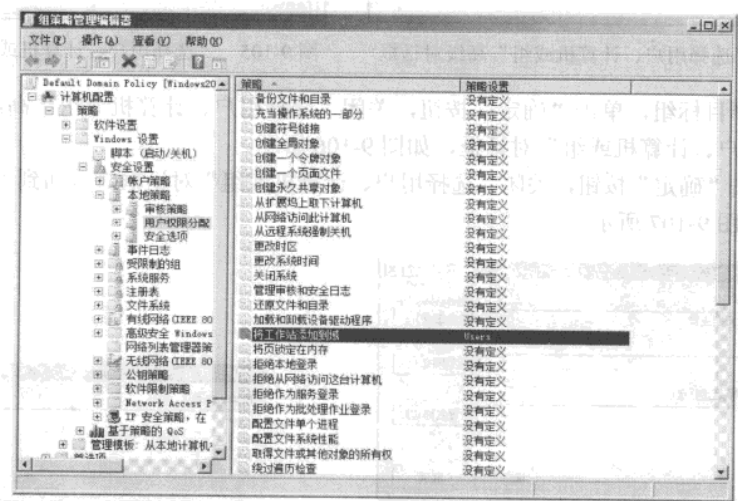


图 9-109 “组策略管理编辑器”窗口

9.4.2 计算机账户生命周期

在域中，计算机账户生命周期主要体现在从进入域到脱离域的全过程。主要经历以下几个阶段：

- (1) 进入域，称之为加域，将客户端计算机添加到 Active Directory 中。
- (2) 活动域账户。
- (3) 脱离域，称之为降域，将客户端计算机脱离域。

1. 升域

Windows 2000 以上操作系统提供多种加入 Active Directory 的方法，包括命令行方式（前提在 Active Directory 中创建计算机）、“网络标识向导”方式和系统属性更改，3 种方式应用的环境不同，完成同样的管理任务。以系统属性更改为例说明。

第 1 步，右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令，弹出“系统属性”对话框，打开“计算机名”选项卡，显示如图 9-110 所示的“计算机名”对话框。

第 2 步，单击“更改”按钮，显示的“计算机名称更改”对话框。在“隶属于”分组区域中，选择“域”单选按钮，在“域”文本框中输入域名，例如 book，如图 9-111 所示。

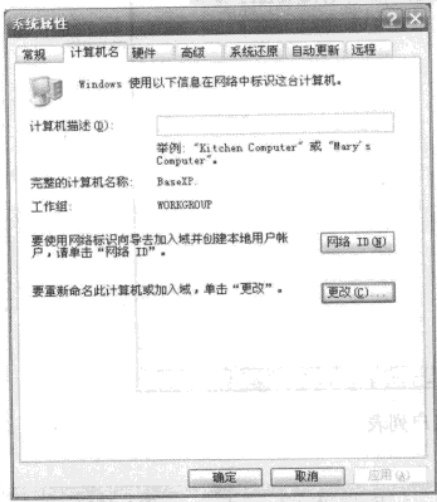


图 9-110 升域之一

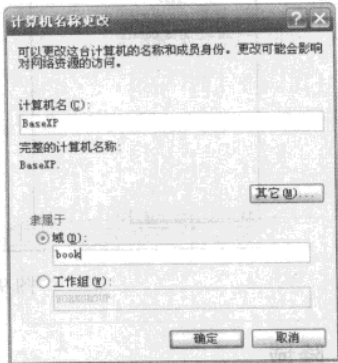


图 9-111 升域之二

第 3 步，单击“确定”按钮，显示如图 9-112 所示的“计算机名更改”对话框。在“用户名”和“密码”文本框中，输入具备将用户添加到域中权限的用户名和密码。

第 4 步，单击“确定”按钮，执行升域操作，执行成功后，显示如图 9-113 所示的“计算机名更改”对话框。单击“确定”按钮，重新启动计算机后即可登录域。

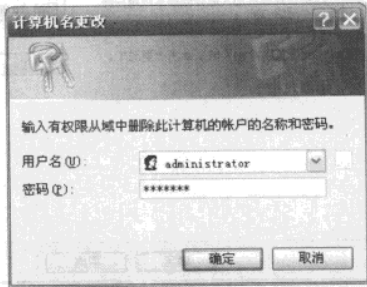


图 9-112 升域之三

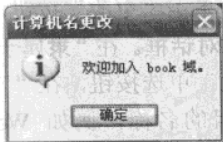


图 9-113 升域之四

2. 活动域账户

客户端计算机加入域后，默认添加在“Computers”组中。所有加入域的计算机（客户端计算机和成员服务器）都添加到此组中，如图 9-114 所示。计算机账户最典型的应用为：在 Active Directory 中分组，将客户端计算机分到不同的组织单位中，通过 WSUS 服务器为不同的客户端计算机分发补丁。

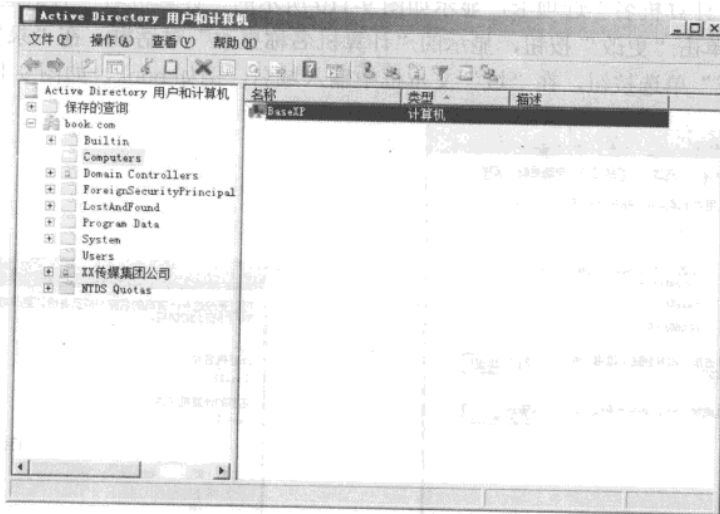


图 9-114 计算机账户列表

3. 降域

计算机损坏或者重新安装操作系统，致使计算机名和以前不同，管理员可以在“Active Directory 用户和计算机”将不再使用的计算机禁用或者删除，建议的方法是将计算机脱离域，自动禁用计算机。

第 1 步，右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，弹出“系统属性”对话框，打开“计算机名”选项卡，显示如图 9-115 所示的“计算机名”对话框。

第 2 步，单击“更改”按钮，显示的“计算机名称更改”对话框。在“隶属于”分组区域中，选择“工作组”单选按钮，在“工作组”文本框中输入工作组的名称，例如 Workgroup，如图 9-116 所示。

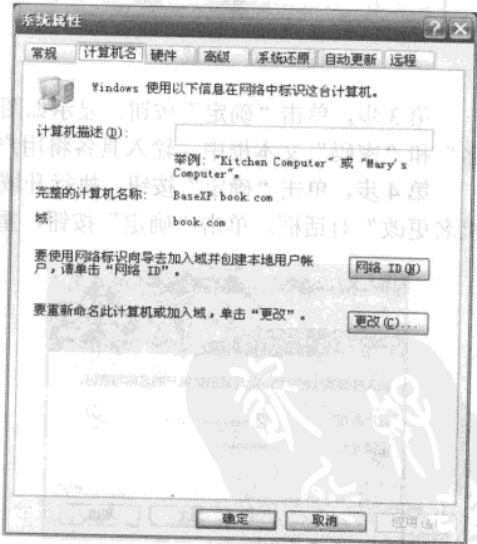


图 9-115 降域之一

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

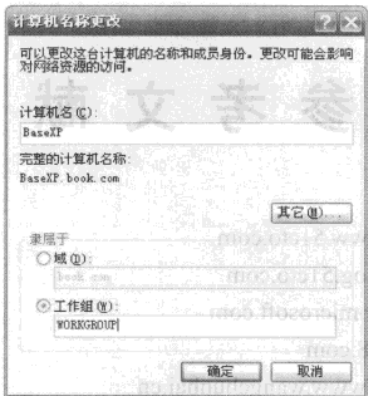


图 9-116 降域之二

第 3 步，单击“确定”按钮，显示如图 9-117 所示的“计算机名更改”对话框。在“用户名”和“密码”文本框中，输入具备降域用户权限的用户名称和密码。

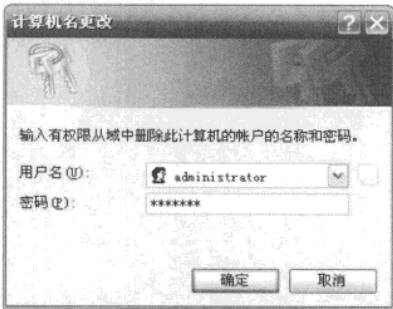


图 9-117 降域之三

第 4 步，单击“确定”按钮，执行降域操作，执行成功后，显示如图 9-118 所示的“计算机名更改”对话框。单击“确定”按钮，重新启动计算机后即可脱离域。

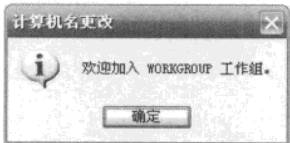


图 9-118 降域之四

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

参考文献

- [1] 51CTO 网站: <http://www.51cto.com>
- [2] 51CTO 博客: <http://blog.51cto.com>
- [3] Microsoft: <http://www.microsoft.com>
- [4] IT168: <http://www.it168.com>
- [5] 王春海的网站: <http://www.wangchunhai.cn>
- [6] 虚拟机之家: <http://www.xuniji.com> 